QA
171
M31p
v.1

ENGINEERING &
MATHEMATICAL
SCIENCES LIBRARY

A
000
648
030
5

UC SOUTHERN REGIONAL LIBRARY FACILITY

THE LIBRARY
OF
THE UNIVERSITY
OF CALIFORNIA
LOS ANGELES

STANFORD UNIVERSITY PUBLICATIONS
UNIVERSITY SERIES

MATHEMATICS AND ASTRONOMY
Volume I Number 1

PRIMITIVE GROUPS

PART I

BY

WILLIAM ALBERT MANNING,
Professor of Applied Mathematics

STANFORD UNIVERSITY, CALIFORNIA
PUBLISHED BY THE UNIVERSITY
1921

STANFORD UNIVERSITY PUBLICATIONS
UNIVERSITY SERIES

MATHEMATICS AND ASTRONOMY

Vol. I.

No. 1. PRIMITIVE GROUPS. William Albert Manning, Professor of Applied Mathematics. 108 pages. Price, $1.25.

The series of monographs issued by Stanford University under the title, "Leland Stanford Junior University Publications, University Series," has been brought to a close. Hereafter the papers in the University Series will be issued in various groups under the general title, "Stanford University Publications, University Series." A list of the papers issued in the old series, giving prices, may be obtained from the Librarian of Stanford University.

STANFORD UNIVERSITY PUBLICATIONS
UNIVERSITY SERIES

MATHEMATICS AND ASTRONOMY
VOLUME I NUMBER 1

PRIMITIVE GROUPS

PART I

BY

WILLIAM ALBERT MANNING,
Professor of Applied Mathematics

STANFORD UNIVERSITY, CALIFORNIA
PUBLISHED BY THE UNIVERSITY
1921

STANFORD UNIVERSITY
PRESS

QA
171
M31p
v.1

Engineering &
Mathematical
Sciences
Library

CONTENTS

CHAPTER I.

The Elementary Theory of Groups of Permutations.

SECTION PAGE
1. Permutations 7
2. The Linear Homogeneous Substitution 10
3. Similar Permutations 12
4. Group of Permutations 14
5. Lagrange's Theorem 16
6. Quotient Groups 17
7. Some Elementary Theorems 20
8. Permutable Groups 22
9. Conjugate Permutations and Conjugate Groups 24
10. Sylow's Theorem 26

CHAPTER II.

Transitive Groups.

11. Transitive Groups.—Homomorphic Groups 28
12. Regular Groups and the Holomorph 30
13. Complete Groups 32
14. Transitive Groups Isomorphic to a Given Group 35
15. A Group Isomorphic to the Symmetric Group 36
16. Definition of Primitive and Imprimitive Groups, of Equivalent and Similar Groups 37
17. The Subgroup that Fixes One Letter of a Transitive Group . . 40
18. An Existence Theorem for Multiply Transitive Groups 41
19. The Average Number of Letters in the Permutations of a Transitive Group 43

CHAPTER III.

Group Characteristics.

20. The Normal Form 45
21. The Open Product 47
22. The Canonical Substitution 49
23. Substitutions Commutative with a Canonical Substitution . . . 51
24. Group of Substitutions 53
25. The Sum of Substitutions 54

876181

SECTION PAGE
26. The Hermitian Form 56
27. The Composition of Two Homomorphic Groups 58
28. The Hermitian Invariant 61
29. The Complete Reduction of a Reducible Group 63
30. Reduction of the Regular Group 65
31. Other Relations Between the Characteristics 68

CHAPTER IV.

Applications of Group Characteristics.

32. Permutation Groups of Degree n and Class $n-1$ 70
33. The Reduction of Transitive Groups 72
34. Groups of Degree n Containing a Circular Permutation of n letters 74
35. Groups of Order $p^{a}q^{\beta}$ 78

CHAPTER V.

Transitive Groups.

36 The Largest Subgroup in which a Given Subgroup or Permutation Is Invariant 81
37. The Transitive Constituents of the Subgroup that Fixes One Letter of a Uniprimitive Group 83
38. Multiply Transitive Constituents of the Subgroup that Fixes One Letter of a Uniprimitive Group 83
39. Invariant Subgroups of Primitive Groups 87
40. Invariant Imprimitive Subgroups of Doubly Transitive Groups . 88
41. Certain Imprimitive Groups 89

CHAPTER VI.

Primitive Groups with Transitive Subgroups of Lower Degree.

42. Introduction 92
43. The Transitive Subgroup 93
44. The Limit of Transitivity 96
45. The Imprimitive Subgroups of a Doubly Transitive Group . . 97
46. The Limit of the Degree of a Primitive Group in Terms of the Degree of a Transitive Subgroup 103
47. Discussion of F_{r-1} When It Has Imprimitive Systems of q_r^2 or $q_r^2 + q_r$ Letters 105
48. The Holomorph of the Elementary Group of Order p^n 107

PREFACE

Some knowledge of Algebraic Numbers and of the ordinary Theory of Numbers is assumed to have been acquired by the reader by way of preparation for a serious study of the subject of which this volume treats.

An apology may be in order for the arrangement of the subject matter. It was arranged as it is to meet the needs of actual instruction. The use of "group characteristics," as developed by Frobenius, should be a familiar tool in the hands of the student as early as possible. Therefore linear substitutions are taken up in the third chapter. From the point of view of strict logic this study of linear substitutions and of linear groups should be quite fully developed before those very special substitutions which we call permutations are considered. But the idea of groups of non-commutative operations can, in the author's opinion, be best gained from a few lessons on the concrete and familiar permutations of a finite number of letters. Therefore the first two chapters are intended to familiarize the learner with the simpler processes used in Group Theory, to exhibit the fundamental theorems which admit of briefly worded proof, and to prepare the way for the more difficult developments of linear groups. Moreover, since any "abstract" group of finite order is isomorphic to some group of permutations, it would seem that sufficient generality can be attained if the phraseology of the abstract theory is ignored, as is done in this book.

In talking of prime numbers it is admitted that it is a matter of indifference whether unity is included among the primes or not. May one be permitted the same license, if for the sake of convenience in stating certain theorems, the identical substitution alone is denied the dignity of being called a group (§ 4)? The new terms "similar groups" (§ 16), "open product" (§ 21) and "uniprimitive group" (§ 37) seem useful and necessary.

In justification of the publication of these pages in our University series, it may be stated that some of the material to be found in the volume is new. In particular theorems II of § 37, I of § 38, and I of § 45 have not been published elsewhere.

Among the sources from which the author has drawn inspiration and material the following treatises should be mentioned:

Jordan, *Traité des substitutions;*
Weber, *Lehrbuch der Algebra;*
Burnside, *Theory of Groups;*

Dickson, *Linear Groups;*
Miller, Blichfeldt and Dickson, *Finite Groups;*
Blichfeldt, *Finite Collineation Groups;*
Hilton, *Linear Substitutions.*

But the memoirs of Jordan and of Frobenius have contributed more by way of suggestion and encouragement than any books.

The author is glad of an opportunity to express his thanks to Professor H. F. Blichfeldt, Professor H. C. Moreno, and Miss Anna L. Wright, who have read parts of the manuscript, and to Mr. H. W. Brinkmann, who has read all of it. Their criticisms and suggestions have been of great value. Nor should the author's great indebtedness to Professor G. A. Miller go unacknowledged. He owes his first advanced knowledge of the subject to Professor Miller's lectures at Stanford University from 1901 to 1906.

W. A. MANNING

CHAPTER I.

The Elementary Theory of Groups of Permutations.

§ 1.

Permutations.

There are $n!$ different ways in which n objects (n a finite integer) may be arranged. If the n objects are tagged by means of n different letters $x_1, x_2, \cdots, x_n$, these arrangements are completely described by the $n!$ permutations of the letters $x_1, x_2, \cdots, x_n$, or what is the same thing, by the $n!$ permutations of the subscripts $1, 2, \cdots, n$. A notation that immediately suggests itself for a *permutation* is this:

$$\begin{pmatrix} x_1 & x_2 & \cdot & \cdot & \cdot & x_n \\ x_1' & x_2' & \cdot & \cdot & \cdot & x_n' \end{pmatrix}$$

where $x_1', x_2', \cdots, x_n'$ are the letters $x_1, x_2, \cdots, x_n$ over again, and this permutation is one in which x_i' replaces x_i $(i = 1, 2, \cdots, n)$. With this notation the n columns may be read in any order. For example,

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_3 & x_4 & x_1 \end{pmatrix} = \begin{pmatrix} x_1 & x_3 & x_4 & x_2 \\ x_2 & x_4 & x_1 & x_3 \end{pmatrix}.$$

A permutation is *circular* if by a rearrangement of its columns every letter of the first row has the same letter next to it on the right as it has under it; we agree that the first column is the right-hand neighbor of the last column.

If this definition is used as a test as to whether a given permutation is circular or not, a negative result declares that the permutation breaks into two or more circular permutations, no two of which have a letter in common. This decomposition is unique. The component circular permutations of two or more letters are called the *cycles* of the permutation.

When a circular permutation is so written that each letter is replaced by the letter on its right, the second row becomes superfluous. Then

$$(x_1 x_2 \cdots x_n)$$

is a briefer notation for the permutation

$$\begin{pmatrix} x_1 & x_2 & \cdot & \cdot & \cdot & x_{n-1} x_n \\ x_2 & x_3 & \cdot & \cdot & \cdot & x_n \ \ x_1 \end{pmatrix}.$$

The circular permutations of three letters x_1, x_2, x_3 are

$$(x_1)(x_2)(x_3),\ (x_1x_2x_3),\ (x_1x_3x_2),\ (x_1)(x_2x_3),\ (x_2)(x_1x_3),\ (x_3)(x_1x_2).$$

The first permutation, $(x_1)(x_2)(x_3)$, leaves the three letters fixed and is called the *identical permutation,* or the *identity;* $(x_1x_2x_3)$ replaces x_1 by x_2, x_2 by x_3 and x_3 by x_1; $(x_1)(x_2x_3)$ fixes x_1 and replaces x_2 by x_3 and x_3 by x_2; that is, it transposes x_2 and x_3.

A circular permutation of two letters is a *transposition.* No difficulty can arise if circular permutations of one letter are omitted when recording a permutation, except in the case of the identity, and for this permutation which fixes each of the n letters in question, the symbol for unity, 1, may be used without ambiguity. Thus even the six permutations of the numbers 1, 2, 3, are written

$$1,\ (123),\ (132),\ (23),\ (13),\ (12).$$

We shall say that a permutation *displaces* a letter when that letter is in a cycle of the permutation.

That permutation which results from two or more successive permutations is called the *product* of those permutations. We agree that the order in which the permutations are carried out is from left to right. Thus if $x_1 + 4x_2 + 5x_3$ is first subjected to the circular permutation (132) and then to the transposition (23), the result is the same as if the single permutation (12) were carried out; that is,

$$(132)(23) = (12).$$

But if the order of these operations is reversed,

$$(23)(132) = (13).$$

Hence:

I. The multiplication of permutations is not always a commutative operation.

It is evident, however, that the product of two permutations that have no letter in common is independent of the order in which they are taken. Furthermore, the associative law,

$$ABC = A(BC),$$

holds for any three permutations A, B, C.

If the same permutation S is carried out k times, the resulting permutation is called the k^{th} *power* of S, and for it the symbol S^k is in common use. The *square* of a permutation is its second power. A permutation is commutative with itself and therefore is commutative with each of its powers. A circular permutation of n letters raised to the n^{th} power is the identity. This is clear if we notice that in the k^{th} power of a circular permutation each letter is followed by the letter which in the original permutation was the k^{th} letter to the right of it.

The *order* of any permutation S is the least positive integer k for which

$$S^k = 1.$$

Therefore the order of S is the least common multiple of the orders of its cycles. Thus $(ab)(cde)$ is of order 6; $(abcd)(efghij)$ is of order 12.

The *inverse* of a permutation S is that permutation which completely undoes the work of S and which therefore is S read backward, from right to left. It is S^{k-1} if S is of order k, or, as it is often written, S^{-1}. The inverse of S^x is S^{k-x}. Thus a meaning is attached to negative integral exponents. The two laws of exponents hold:

$$S^x S^y = S^{x+y},$$

$$(S^x)^y = S^{xy},$$

where we may reduce, if we like, all exponents modulo k, k being the order of S.

Let there be given two permutations, S and T. The product

$$S^{-1}TS$$

is of very frequent occurrence and is called the *transform* of T by S. It reduces to T if S and T are commutative.

II. The permutation $S^{-1}TS$ may be written down by putting in place of each letter of T that letter which follows it in S.

To prove this, let $(abc \cdots m)$ be any cycle of T and let

$$S = \begin{pmatrix} a\,b\,c & \cdots & m & \cdots \\ a'b'c' & \cdots & m' & \cdots \end{pmatrix}.$$

Then

$$S^{-1} = \begin{pmatrix} a'b'c' & \cdots & m' & \cdots \\ a\,b\,c & \cdots & m & \cdots \end{pmatrix},$$

and

$$S^{-1}TS = (a'b'c' \cdots m') \cdots.$$

Thus to every cycle of T there corresponds a cycle of $S^{-1}TS$, which is merely the result of carrying out the permutation S upon that cycle of T.

§ 2.

The Linear Homogeneous Substitution.

The meaning of the transform will become clearer if we give some attention to the *linear homogeneous substitution*

$$T: \qquad x_i = \sum_{j=1}^{n} a_{ij} x'_j \qquad (i = 1, 2, \cdots, n).$$

The variables and coefficients of T are ordinary complex numbers.

Suppose that we wish to change the variables of T by means of a second substitution:

$$S: \qquad x_m = \sum_{k=1}^{n} b_{mk} y_k \qquad (m = 1, 2, \cdots, n),$$

and what is the same thing,

$$x'_m = \sum_{k=1}^{n} b_{mk} y'_k \qquad (m = 1, 2, \cdots, n).$$

We obtain

$$\sum_{k=1}^{n} b_{ik} y_k = \sum_{j=1}^{n} a_{ij} \sum_{s=1}^{n} b_{js} y'_s$$

$$= \sum_{j=1}^{n} \sum_{s=1}^{n} a_{ij} b_{js} y'_s \qquad (i = 1, 2, \cdots, n).$$

Multiply by B_{it}, the minor of b_{it} in the determinant

$$B = |b_{mk}|$$

of S and sum:

$$\sum_{i=1}^{n} B_{it} \sum_{k=1}^{n} b_{ik} y_k = \sum_{i=1}^{n} B_{it} b_{it} y_t = B y_t$$

$$= \sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{s=1}^{n} B_{it} a_{ij} b_{js} y'_s.$$

If the determinant of the substitution S is not zero, we have the transformed substitution

$$y_t = \sum_{s=1}^{n} c_{ts} y'_s \qquad (t = 1, 2, \cdots, n),$$

where

$$c_{ts} = \sum_{i=1}^{n} \sum_{j=1}^{n} B_{it} a_{ij} b_{js} / B.$$

But this is the result of making in succession the three substitutions:

$$S^{-1}: \qquad y_t = \sum_{i=1}^{n} z_i B_{it} / B \qquad (t = 1, 2, \cdots, n),$$

$$T: \qquad z_i = \sum_{j=1}^{n} a_{ij} z'_j \qquad (i = 1, 2, \cdots, n),$$

$$S: \qquad z_j = \sum_{s=1}^{n} b_{js} y'_s \qquad (j = 1, 2, \cdots, n).$$

The result of making first the substitution T and then the substitution S may be brought about by means of the third substitution

$$z_i = \sum_{j=1}^{n} \sum_{k=1}^{n} a_{ij} b_{jk} z'_k \qquad (i = 1, 2, \cdots, n).$$

This substitution is called the *product* TS.

A permutation is a substitution of determinant ± 1 with coefficients all zero in each row (or column) but one, and that coefficient is unity. Hence when we multiply out the product $S^{-1}TS$ we really are making in T that change of variables indicated by S.

While it was found necessary to assume above that the determinant of the substitution S was not zero, no condition was placed upon the determinant of T.

It appears from the product:

$$z_i = \sum_{j=1}^{n} \sum_{k=1}^{n} a_{ij} b_{jk} z'_k \qquad (i = 1, 2, \cdots, n),$$

that the determinant of TS is the product of the determinants of T and S. Hence $S^{-1}TS$ and T have the same determinant if the determinant of S is not zero.

Again,

$$\begin{aligned} \sum_{k=1}^{n} c_{kk} &= \sum_{k=1}^{n} \sum_{i=1}^{n} \sum_{j=1}^{n} B_{ik} a_{ij} b_{jk} / B \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} \sum_{k=1}^{n} B_{ik} b_{jk} / B \\ &= \sum_{i=1}^{n} a_{ii}. \end{aligned}$$

The sum of the coefficients in the principal diagonal of a substitution T is called the *characteristic* of the substitution T. These two results may be stated in the theorem:

I. The determinant and the characteristic of a substitution T are invariant under transformation by a substitution S of non-zero determinant.

§ 3.

Similar Permutations.

Two permutations S and T are said to be *similar* if a third permutation X exists that satisfies the equation

$$X^{-1}SX = T.$$

No solution is possible unless S and T have the same number of cycles of any given order. But when this condition is satisfied, if T be written in a line below S, with a cycle of T below a cycle of the same order of S, then a permutation of the letters displaced by S and T jointly that has the required property may be set up by continuing the row in which S stands with those letters of T that are fixed by S, and by continuing the second row until it also has as many letters as the first by means of the letters of S that are fixed by T. For example, one permutation that transforms $(ab)(cde)$ into $(fc)(abe)$ is

$$\begin{pmatrix} abcdef \\ fcabed \end{pmatrix} = (afdbc).$$

A permutation is *regular* if all its cycles are of the same order. Any power of a circular permutation is regular.* Two regular permutations are similar if they displace the same number of letters and are of the same order.

The equation

$$X^{-1}SX = T$$

has then either no solution or an infinite number of solutions. But those solutions which displace only the letters of S and T may well be called the *principal solutions.* If S and T are similar and regular, with h cycles of α letters each, the number of principal solutions of $X^{-1}SX = T$ is exactly $\alpha^h h!$. If S and T are similar but not regular, each may be regarded as the product of k regular permutations made up of h_i cycles of α_i letters each $(i = 1, 2, \cdots, k)$. Then the number of principal solutions is seen to be

$$\prod_{i=1}^{k} \alpha_i^{h_i} h_i!$$

In particular the number of principal solutions of

$$X^{-1}SX = S,$$

where S is a circular permutation of prime order p, is p, and evidently these p permutations are the powers of S. Again there are just p principal solutions of the equation

* Conversely any regular permutation is some power of a circular permutation.

$$X^{-1}SX = S^{m} \quad (m \not\equiv 0,\ m \not\equiv 1,\ \text{mod } p)\,.$$

Each of these solutions fixes one and only one letter of S. Take one of these solutions. Then

$$\begin{aligned} X^{-2}SX^{2} &= X^{-1}S^{m}X \\ &= X^{-1}SXX^{-1}SX \cdots \text{(to } m \text{ factors)} \\ &= (S^{m})^{m} = S^{m^2}, \\ X^{-3}SX^{3} &= X^{-1}S^{m^2}X = S^{m^3}, \\ &\cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ X^{-n}SX^{n} &= S^{m^n}. \end{aligned}$$

Now if n is the exponent of the lowest power of X for which

$$X^{-n}SX^{n} = S,$$

we have

$$S^{m^n} = S;$$

and since X is of degree $p-1$,

$$X^{n} = 1.$$

Then

$$m^{n} \equiv 1, \quad \text{mod } p\,.$$

Hence, if m is a primitive root of the congruence

$$x^{p-1} \equiv 1, \quad \text{mod } p\,,$$

the permutation X that transforms S into S^{m} is of order $p-1$ and all the permutations we have been seeking are given by the $p(p-1)$ products

$$S^{y}X^{z} \quad (y = 1, \cdots, p;\ \ z = 1, 2, \cdots, p-1).$$

The product of any two of these $p\ (p-1)$ permutations is again one of them, since

$$S^{a}X^{b}S^{c}X^{d} = S^{a+cm^{-b}}X^{b+d}\,.$$

These $p(p-1)$ permutations may be compactly expressed by

$$\begin{pmatrix} x \\ x' \end{pmatrix}$$

as a permutation of the p incongruent residues 0, 1, $\cdots$, $p-1$, if

$$x' \equiv ax + b\,, \quad \text{mod } p\,,$$

where a and b are allowed to assume the p values $0, 1, \cdots, p-1$, with the exception that

$$a \not\equiv 0, \quad \text{mod } p.$$

§ 4.

Group of Permutations.

Certain distinct permutations of a finite number of letters constitute a *group* if the product of any two (or the square of any one) of them is one of the given permutations.

This definition requires the presence of at least two permutations in any group. The identity alone, by our convention, is not a group.

The $n!$ permutations of n ($\geqq 2$) letters necessarily satisfy this definition. This is the *symmetric* group. The number of letters displaced by the permutations of a group is its *degree*. The total number of permutations in a group is its *order*.

One group is a *subgroup* of another when all its permutations are permutations of the second, and its order is less than the order of the second. Thus the symmetric group of degree n includes as subgroups all other groups that do not displace one or more other letters. It includes itself, of course, but not as a subgroup.

A group is *cyclic* when all its permutations are powers of one of its permutations. Thus

$$1,\ (ab)$$

is a cyclic group of order 2;

$$1\,,\ (ab)(cde)\,,\ (ced)\,,\ (ab)\,,\ (cde)\,,\ (ab)(ced)$$

is a cyclic group of order 6. The cyclic group

$$1,\ (123),\ (132)$$

is a subgroup of the symmetric group

$$1,\ (123),\ (132),\ (12),\ (13),\ (23).$$

One or more permutations are said to *generate* a group if every permutation of the group is a product whose factors are some or all of these *generators*. The same permutation may recur at different places as a factor of this product if the generating permutations are not commutative. By the notation

$$\{S\,,\,T\,,\cdots\}$$

is meant the group generated by the permutations S, T, $\cdots$. Then $\{S\}$ is a cyclic group of order k if S is of order k. The word *degree* will sometimes be used of a permutation, meaning thereby the number of letters it displaces, that is, the degree of the cyclic group it generates.

Any circular permutation is a product of transpositions, as

$$\begin{aligned}(123 \cdots mn) &= (12)(13)(14) \cdots (1m)(1n)\\ &= (1n)(nm)(ml) \cdots (43)(32)\\ &= \text{etc.}\end{aligned}$$

Hence any permutation is a product of transpositions which displace no letter not displaced by the permutation in question. In other words, *a symmetric group is generated by its transpositions.* Now any permutation of n letters $x_1, x_2, \cdots, x_n$ must transform

$$\prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (x_i - x_j)$$

into itself or into its negative, because this product is the square root of a symmetric function. An odd number of transpositions changes its sign and an even number of transpositions leaves it invariant. Therefore, although a permutation can be written as a product of transpositions in a number of ways, it is always equal to the product of an odd number or an even number of transpositions and is called a *negative* or a *positive* permutation in the two cases, respectively. Since the determinant of a transposition is -1, negative permutations are of determinant -1 and positive permutations are of determinant $+1$.

I. If a group contains a negative permutation, just half its permutations are positive.

There is at least one positive permutation in any group, the identity. If

$$S_1, S_2, S_3, \cdots S_h \quad (h > 1)$$

are the positive permutations of the given group G, and if T is a negative permutation of G (by hypothesis there is at least one such), all the permutations

$$S_1T, S_2T, S_3T, \cdots, S_hT$$

are negative. It is necessary to show that these h negative permutations are distinct and that there are no other negative permutations in G.

If

$$S_iT = S_jT,$$

$$S_iTT^{-1} = S_jTT^{-1},$$

whence, by the associative law,

$$S_i(TT^{-1}) = S_j(TT^{-1}),$$

and finally

$$S_i = S_j.$$

If U is any negative permutation of the group, UT^{-1} is a positive permutation:

$$UT^{-1} = S_k,$$

and therefore

$$U = S_k T.$$

A consequence of this theorem is that a symmetric group of degree n (> 2) has a subgroup of order $n!/2$ all the permutations of which are positive. For the product of two positive permutations is positive. This is the *alternating* group. It contains no transpositions, but its permutations of lowest degree are circular permutations of three letters.

The alternating group of degree 4 has permutations of order 3 which are distributed among four subgroups of order 3, and three permutations of order 2 and degree 4 which with the identity constitute a subgroup of order 4, known as the *axial* group.

§ 5.

Lagrange's Theorem.

When two permutations leave the same letter a fixed, their product also leaves a fixed. Therefore the permutations that leave the same letter of any group fixed constitute a subgroup. One subgroup of the symmetric group of degree n (> 2) is the symmetric group of degree $n - 1$.

I. The order of a group is divisible by the order of any subgroup.

Let H be any subgroup of a group G of order g. Let

$$S_1, S_2, \cdots, S_h$$

be the permutations of H, and let T_2 be a permutation of G not in H. There is such a permutation, because g is greater than h by the definition of a subgroup. Consider the permutations

$$S_1T_2, S_2T_2, \cdots, S_hT_2.$$

None of them are in H, for if

$$S_i = S_jT_2,$$

$$T_2 = S_j^{-1}S_i.$$

Nor is

$$S_kT_2 = S_mT_2$$

for then

$$S_k = S_m.$$

If there are no more permutations in G, the theorem is proved. Let there be another permutation T_3 distinct from each of the $2h$ permutations above. Write the products

$$S_1T_3\,,\ S_2T_3\,,\cdots,\ S_hT_3\,.$$

As before, no

$$S_iT_3 = S_jT_3\,,$$

nor is

$$S_iT_3 = S_k\,.$$

If

$$S_iT_3 = S_jT_2\,,$$

then

$$T_3 = S_i^{-1}S_jT_2\,,$$

contrary to hypothesis. If the permutations of the group are not exhausted, continue this process until no more remain. Since G is a group of permutations it is of finite order. We shall have therefore a last row

$$S_1T_{g/h}\,,\ S_2T_{g/h}\,,\cdots,\ S_hT_{g/h}\,,$$

in which no two permutations are the same, nor is any permutation of this row the same as a permutation in a row above it. Hence g/h is a whole number. The quotient g/h is sometimes called the *index* of the subgroup H.

In the course of the above proof we have shown once for all that

II. If H is any subgroup of G and if T_i is a permutation of G not in one of the $i-1$ rows above it, the permutations of the row

$$S_1T_i\,,\ S_2T_i\,,\cdots,\ S_hT_i$$

are distinct from each other and occur in no preceding row.

A condensed notation for the i^{th} row of the array is

$$HT_i\,,$$

where for H each permutation of H is to be written in turn. We shall also use this notation for the product of any one permutation of H into a certain permutation of T_i.

The array could just as well have been written

$$T'_iH\,,$$

where T'_i is a permutation of G not in a row above the i^{th}.

§ 6.

Quotient Groups.

The group H is said to be transformed into itself by a permutation T when every permutation

$$T^{-1}S_1T,\ T^{-1}S_2T\ \cdot\cdot\cdot,\ T^{-1}S_hT$$

is a permutation of H. This is often written symbolically

$$T^{-1}HT = H.$$

A subgroup H of a group G is *self-conjugate* (or *invariant*) in G when every permutation of G transforms H into itself. If G has no self-conjugate subgroup, it is a *simple* group. For example, cyclic groups of prime order are simple.

We have just been studying the group G with its permutations arranged in the g/h rows

$$(1) \qquad HT_i \qquad (i=1, 2, \cdots, g/h).$$

When H is an invariant subgroup of G,

$$HT_i = T_iH,$$

and therefore

$$HT_iHT_j = HT_iT_j = HT_k\,.$$

This means that if (1) be multiplied on the right by the g/h permutations $S'T_1, S''T_2, \cdots$, where $S', S'', \cdots$ are any permutations of H, thus:

$$\begin{array}{llll} HT_1, & HT_2, & \cdots, & HT_{g/h}, \\ HT_1T_2, & HT_2T_2, & \cdots, & HT_{g/h}T_2, \\ \cdot & \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot \\ HT_1T_{g/h}, & HT_2T_{g/h}, & \cdots, & HT_{g/h}T_{g/h}, \end{array}$$

the new array so formed displays g/h distinct permutations of the g/h rows $HT_1, HT_2, \cdots$ of G. They are tagged for us by the subscripts $1, 2, \cdots$ of $T_1, T_2, \cdots$. The product of the two permutations

$$\begin{pmatrix} HT_i \\ HT_iT_j \end{pmatrix} \qquad (i=1, 2, \cdots, g/h)$$

and

$$\begin{pmatrix} HT_u \\ HT_uT_k \end{pmatrix} \qquad (u=1, 2, \cdots, g/h)$$

is

$$\begin{pmatrix} HT_i \\ HT_i(T_jT_k) \end{pmatrix}.$$

Hence the g/h rows of G, by right hand multiplication by the permutations of G, when H is an invariant subgroup of order h, are permuted according to the permutations of a group of degree and order g/h. This group is called the *quotient-group* of G with respect to H and for it there is a convenient symbol:

$$G/H.$$

If now beside each row HT_j of G we write the permutation

$$\begin{pmatrix} HT_i \\ HT_iT_j \end{pmatrix},$$

to the product of any permutation of HT_j by any permutation of HT_k there corresponds uniquely the product

$$\begin{pmatrix} HT_i \\ HT_i(T_jT_k) \end{pmatrix}.$$

Hence the theorem:

I. To any subgroup of order λ in G/H there corresponds a subgroup of order $h\lambda$ in G. The order of any permutation of G is divisible by the order of the corresponding permutation of G/H.

It does not follow that G always has a subgroup of order g/h with one permutation from each row of HT_i. After proving the following theorem we shall set up a group in confirmation of this statement.

II. If a permutation T transforms a group H of order h into itself, and if the lowest power of T that is in H is the k^{th}, then $\{H, T\}$ is a group of order hk.

The proof follows the same lines as before. Write the permutations of H in a row and complete a rectangular array by multiplying them by $k-1$ powers of T:

$$\begin{array}{llll}
S_1, & S_2, & \cdot\ \cdot\ \cdot, & S_h, \\
S_1T, & S_2T, & \cdot\ \cdot\ \cdot, & S_hT, \\
S_1T^2, & S_2T^2, & \cdot\ \cdot\ \cdot, & S_hT^2, \\
\cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \\
S_1T^{k-1}, & S_2T^{k-1}, & \cdot\ \cdot\ \cdot, & S_hT^{k-1}.
\end{array}$$

If

$$S_iT^m = S_jT^n \qquad (n \leqq m < k),$$

$$T^{m-n} = S_i^{-1}S_j,$$

which is impossible unless $m = n$ and $i = j$. Hence the hk permutations of the above array are all different. Again, any permutation S_iT^x $(x \geqq k)$ may be written

$$S_iT^{qk+r} = S_iS_jT^r,$$

where the remainder r is less than k. It remains to show that any permutation $S_iT^uS_jT^v$ may be reduced to S_wT^x. The condition that T transforms H into itself gives the means for doing this:

$$T^{-1}S_aT = S_b,$$

and by successive transformations by T,

$$T^{-u}S_aT^u = S_c,$$

whence

$$T^uS_c = S_aT^u.$$

Applying this to $S_iT^uS_jT^v$, we replace T^uS_j by S_kT^u, and then have

$$S_iT^uS_jT^v = S_iS_kT^{u+v}.$$

Therefore the hk permutations of the array form a group, and since this group includes both H and T, it is the group $\{H, T\}$.

For example, let H be the cyclic group

$$\{(1234)(5678)\}.$$

The permutation

$$T = (1537)(2846)$$

transforms H into itself and its square is in H. Therefore

$$\{(1234)(5678), (1537)(2846)\}$$

is a group of order 8. It is the *quaternion* group. All the permutations of the row HT are of order 4.

Let H be the axial group

$$1, (12)(34), (13)(24), (14)(23).$$

The permutation

$$T = (1234)$$

transforms H into itself, and

$$T^2 = (13)(24).$$

This group

$$\{(12)(34), (1234)\}$$

is known as the *octic* group.

§ 7.

Some Elementary Theorems.

I. A subgroup of index 2, when one occurs in a group, is self-conjugate.

Let the group G of order g have in it a subgroup H of order $g/2$. If t is a permutation of G but not included in H, then the permutations

$$H, Ht$$

are all distinct, and coincide with the permutations of G. Hence

$$t^{-1}Ht = H.$$

In particular, the alternating group of degree n is invariant in the symmetric group of degree n.

A group is called *Abelian* if any two of its permutations are commutative. For example, cyclic groups are Abelian.

II. A cyclic group G of order g has one and only one subgroup whose order is any divisor $(<g)$ of g.

Let h be any divisor $(< g)$ of g. Then $\{S^{g/h}\}$ is one subgroup of order h. Hence there are at least $\varphi(h)$ permutations of order h in G. Since

$$\sum_{h=1}^{g} \varphi(h) = g\,,$$

there are exactly $\varphi(h)$ permutations of order h and therefore only one subgroup of order h.

It follows that if

$$g = \prod_{i=1}^{\lambda} p_i^{\alpha_i}\,,$$

where $p_1, p_2, \cdots, p_\lambda$ are distinct prime numbers, G has a cyclic subgroup of order

$$p_i^{\alpha_i} \qquad (i = 1, 2, \cdots, \lambda)\,,$$

and G may be generated by its λ subgroups of order $p_i^{\alpha_i}$.

III. If the order of every permutation of a group divides 2, the group is Abelian.

Let S and T be any permutations of a group G. By hypothesis

$$S^2 = T^2 = (ST)^2 = 1\,.$$

Now if

$$STST = 1\,,$$

$$S^2TST^2 = ST\,,$$

that is,

$$TS = ST\,.$$

IV. Two permutations of order 2 whose product is of order h (> 1) generate a group of order $2h$, in which there is an invariant cyclic subgroup of order h.

Let S and T be the two permutations of order 2. We have

$$S^2 = T^2 = (ST)^h = 1.$$

Both S and T transform ST into its inverse: for

$$S^{-1}STS = TS$$

and

$$T^{-1}STT = TST^2 = TS\,;$$

and finally

$$(ST)(TS) = ST^2S = S^2 = 1,$$

so that TS is the inverse of ST.

Hence the cyclic group $\{ST\}$ is transformed into itself by S and, by § 6, II, $\{ST, S\}$ is of order $2h$. Since $\{ST, S\}$ contains $SST = T$, $\{ST, S\}$ coincides with $\{S, T\}$.

Such groups, generated by two distinct permutations of order 2, are called *diedral groups.*

V. All the h permutations not in the cyclic subgroup $\{ST\}$ *of order h of a diedral group are of order 2 and all transform ST into its inverse.*

Now S transforms ST into TS, and therefore transforms $(ST)^x$ into $(ST)^{-x}$. Hence

$$(ST)^xS(ST)^xS=(ST)^x(ST)^{-x}=1.$$

This proves that the h permutations not in $\{ST\}$ are of order 2.

Again,

$$[(ST)^xS]^{-1}ST[(ST)^xS]=S(ST)^{-x}(ST)(ST)^xS=SSTS=TS.$$

The axial group, the symmetric group of degree 3, and the octic group are diedral groups. The diedral group of degree 5 and order 10 is

$$\{(12)(34),\ (23)(45)\}.$$

VI. The permutations (two or more) common to two groups constitute a group.

For the product of two such permutations is in both groups.

This group in which are all the permutations common to two groups, is known as the *cross-cut* of the two groups. If the only common permutation is the identity, there is no cross-cut.

VII. If a group G is transformed into itself by all the permutations of a group H, then K, the cross-cut of G and H, is invariant in H.

Since H transforms G into G, it transforms K into a subgroup K' of G. But K' must also be a subgroup of H, so that

$$K=K',$$

and K is therefore an invariant subgroup of H.

§ 8.

Permutable Groups.

Two groups G and H are said to be *permutable* when, s and t being any two given permutations of G and H, respectively, two other permutations s' and t' of G and H can be found to satisfy the equation

$$st=t's'.$$

We may symbolize this relation thus:

$$GH=HG.$$

For example, a group is permutable with any of its subgroups, for if H is a subgroup of G, we may write G either as

$$H\,,\ Hs_2\,,\ \cdots,\ Hs_n\,,$$

or

$$H\,,\ s_2'H\,,\ \cdots,\ s_n'H\,.$$

I. If G of order g and H of order h are permutable groups with k common permutations, $\{G\,,H\}$ is of order gh/k.

In the following array the first row is G and the first column is H; K is the identity or the cross-cut of G and H:

$$\begin{array}{llll}
K\,, & Ks_2\,, & \cdots, & Ks_{g/k}\,, \\
Kt_2\,, & Ks_2t_2\,, & \cdots, & Ks_{g/k}t_2\,, \\
\cdot & \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot \\
Kt_{h/k}\,, & Ks_2t_{h/k}\,, & \cdots, & Ks_{g/k}t_{h/k}\,.
\end{array}$$

Let $\sigma_1, \sigma_2, \cdots, \sigma_k$ be the permutations of K. Since

$$\sigma_i\ t_j \neq \sigma_u s_w t_v \qquad (v \leqq j)$$

unless

$$\sigma_u s_w = \sigma_i \sigma_r\,,$$

these gh/k permutations are all distinct. Consider the product of any two of them, and apply the condition that G and H are permutable:

$$\sigma_i s_j t_m \sigma_r s_u t_v = \sigma_i s_j \sigma_a s_h \sigma_c t_d t_v = \sigma_x s_y t_z\,.$$

It is therefore one of the permutations of the array and the gh/k permutations are a group in which G and H are subgroups. Therefore $\{G\,,H\}$ is of order gh/k.

In the above proof the condition that G and H are permutable was not used to show that the number of distinct permutations in the array GH is gh/k. This suggests the theorem:

II. If the groups G and rHr^{-1} have exactly k common permutations, the array GrH contains gh/k distinct permutations.

To complete the proof of this theorem it is only necessary to remark that the number of distinct permutations in the array $GrHr^{-1}$ is not changed if each of the gh/k permutations is multiplied by the same permutation r.

Attention should be called to two important special cases of Theorem I, besides II of § 6:

III. If every permutation of G transforms H into itself and every permutation of H transforms G into itself, and if G and H have no cross-cut, every permutation of G is commutative with every permutation of H.

The group $\{G\,,H\}$ is then called the *direct product* of G and H. To prove that $st = ts$, where s and t are any permutations of G and H, respectively, it is only necessary to call attention to the fact that

$$s^{-1}t^{-1}st = 1 .$$

For this permutation is the product of s^{-1} and a permutation of G and is therefore in G; it is the product of $s^{-1}t^{-1}s$, a permutation of H, and t, and is therefore in H. Consequently $s^{-1}t^{-1}st$ is in both G and H and is therefore the identity.

An example of a direct product is the group of order p^2 generated by two commutative permutations of order p, as

$$\{(a_1\ a_2 \cdots a_p)\ ,\ (b_1\ b_2 \cdots b_p)\} .$$

IV. If every permutation of G transforms H into itself, and if every permutation of H transforms G into itself, their cross-cut K is invariant in G and H, and $\{G , H\}/K$ is the direct product of G/K and H/K (on h and g different sets of letters, respectively).

If s and t correspond to different permutations of $\{G , H\}/K$, $s^{-1}t^{-1}st$ belongs to K, which, according to III, proves the theorem.

§ 9.

Conjugate Permutations and Conjugate Groups.

Two permutations (groups, functions) are said to be *conjugate under a certain group G* if G contains a permutation that transforms the one into the other. In particular one conjugate of Σ (any permutation, group, or function) is Σ itself, into which it is transformed by the identity.

A *complete set of conjugates under G* is the totality of permutations (groups, functions) conjugate, under transformation by the permutations of G, to a given permutation (group, function). The phrase "under G" is often omitted when there is no room for doubt as to the group membership of the transforming permutations.

I. The order of any group G is the product of the number of permutations of G by which Σ, a given permutation (group, function), is transformed into itself, and the number of conjugates under G in the complete set to which Σ belongs.

If Σ is transformed into itself by two permutations of G it is transformed into itself by their product, and therefore the permutations of G which transform Σ into itself constitute a subgroup of G, or are G itself. Of course, the theorem requires no proof when Σ is transformed into itself by every permutation of G.

Let I be the largest subgroup of G under which Σ is invariant, or in default of such a subgroup, the identity. By the phrase, *invariant under I,* is meant that every permutation of I transforms Σ into itself. Let s_2 be in G but not in I. All the permutations of the row Is_2 transform Σ into the same permutation (group, function) Σ_2. For

$$s_2^{-1}I^{-1}\Sigma I s_2 = s_2^{-1}\Sigma s_2 = \Sigma_2 .$$

If I and Is_2 do not exhaust the permutations of G, consider Is_3, where s_3 is in neither I nor Is_2. Now $s_3^{-1}\Sigma\, s_3$ is not Σ. Can it be Σ_2? If so, since

$$s_2\Sigma_2 s_2^{-1} = \Sigma ,$$

$$s_2 s_3^{-1}\Sigma s_3 s_2^{-1} = s_2\Sigma_2 s_2^{-1} = \Sigma ,$$

and therefore

$$s_2 s_3^{-1} = I ;$$

that is,

$$s_3 = Is_2 ,$$

contrary to hypothesis. Then the permutations of G may be written in just as many rows

$$Is_i \qquad (i = 1, 2, \cdots, h),$$

as Σ has conjugates under G.

II. If the order of a group is a power of a prime (p^m) it has at least p invariant permutations.

The number of permutations in each complete set of conjugate permutations is a power of the prime p, and one set consists of the identity alone. Then the permutations of the group may be enumerated by counting and adding the number of permutations in each set of conjugates, giving

$$p^m = 1 + p^a + p^b + \cdot \ \cdot \ \cdot ,$$

which is impossible unless at least $p - 1$ of the exponents $a, b, \cdots$ are zero.

For example, (12)(34) is an invariant permutation of the octic group $\{(13)(24),\ (12)\}$.

In any non-Abelian group the invariant permutations, when there are more than one, constitute an invariant subgroup, since the product of two invariant permutations is invariant. The subgroup in which all the invariant permutations and no others are included is the *central* of the group.

To illustrate the application of this theorem, we may prove:

III. A non-cyclic group of order p^2 is the direct product of two groups of order p.

In such a group G all the permutations are of order p, and the preceding theorem assures us that there is a subgroup A of order p in which each permutation is invariant in G. Any other subgroup B of order p generates with A a direct product of order p^2, that is, G.

§ 10.

Sylow's Theorem.

I. If the order g ($>p^m$; p a prime) of a group G is divisible by p^m (>1), G has a subgroup of order p^m.

Assume the truth of the theorem for all groups of order less than g. Our task, then, is to show that G has a subgroup whose order is divisible by p^m.

First, let G be non-Abelian, and let there be γ invariant permutations in G. Let the remaining permutations of G be in complete sets of conjugates of $h_1, h_2, \cdots, h_n$ members. Then

$$g = \gamma + h_1 + h_2 + \cdots + h_n .$$

If γ is not divisible by p, at least one of the numbers $h_1, h_2, \cdots, h_n$ is not divisible by p, whence (§ 9, I) G has a subgroup whose order is divisible by p^m. If γ is divisible by p^x, $(0 < x < m)$, the central of G has a subgroup Δ of order p^x, invariant in G. By hypothesis G/Δ has a subgroup of order p^{m-x} and therefore (§ 6, I) G has a subgroup of order p^m.

If G is Abelian it has a cyclic subgroup A of some prime order q. If $q \neq p$, G/A has a subgroup of order p^m and therefore G contains a permutation of order p (§ 6, I). With $m \geqq 2$, let $q = p$. Then G/A has a subgroup of order p^{m-1} and G has a subgroup of order p^m.

The theorem is true when $g = p^2$ (§ 9, III). Hence it is universally true.

If p^a is the highest power of the prime p that divides the order g ($> p^a$) of G, any subgroup of G of order p^a is called a *Sylow subgroup* of G.

II. Let the order of G be divisible by at least two distinct primes. If there is in G a subgroup H of order p^m which is not included in a subgroup of order p^n ($n > m$), then the subgroups of order p^m are all conjugate in G, their number is congruent to unity, modulo p, and each is a Sylow subgroup of G.

Let H' be any other subgroup of order p^m. These groups H and H' are not permutable, for then H would be contained in a subgroup of G of order p^n ($n > m$). Then (§ 9, I) H' is one of p^a (>1) conjugates under H. If there is another subgroup H'' conjugate to H' under G, it is transformed by H into p^b conjugates distinct from the preceding, and so on. Thus H' is one of $kp + 1$ or kp conjugate subgroups of G, as H

is or is not conjugate to H'. In either case H is one of $rp + 1$ conjugate subgroups (r a positive integer or zero). Since H by hypothesis cannot be invariant in a subgroup of G whose order is divisible by p^{m+1}, it follows (§ 9, I) that p^m is the highest power of p that divides g. But if H' is a Sylow subgroup of G, the number of conjugates in the set to which H' belongs is relatively prime to p. Therefore every subgroup of order p^m is conjugate to H.

This implies that

III. Any subgroup of order p^m of a group whose order is divisible by two or more distinct primes is included in a Sylow subgroup.

We use III to prove the theorem:

IV. Let G be a group of degree n ($\geqq pq$) that contains no permutation of prime order p with so few as q cycles. Let p^a, p^b be the highest powers of p that divide n! and (pq)! respectively. Then the Sylow subgroup of G corresponding to p is not of higher order than p^{a-b}.

Suppose the order of the Sylow subgroup of G is p^{a-b+k}. The Sylow subgroup of the symmetric group of degree n which includes this group of order p^{a-b+k} contains also a subgroup of order p^b, the Sylow subgroup of the symmetric group of degree pq. Since these two subgroups, of orders p^{a-b+k} and p^b, have no permutation except the identity in common they generate the Sylow subgroup of the symmetric group of degree n, and k is necessarily zero.

For example, if a group of degree n contains no permutation of degree less than $u + 1$ except the identity, its order, divides $n!/u!$.

V. In a group of order p^m every subgroup of order p^{m-1} is invariant.

Let H be a subgroup of order p^{m-1} of a group G of order p^m. If H is not invariant it is one of exactly p conjugates under G. But if H' is a subgroup conjugate to H, the latter is one of p subgroups of G conjugate under H', each distinct from H'. This being impossible, H is invariant in G.

VI. In a group of order p^m, every subgroup of order p^n ($n < m - 1$) is included in a subgroup of order p^{n+1}.

Let H be the subgroup of order p^n of the group G of order p^m. It is sufficient to show that H is a subgroup of a subgroup of G. This is certainly the case if H is invariant in G (§ 6, I). Then we may assume that no permutation of G, not in H, transforms H into itself. Let H' be a conjugate of H. Then H' is one of p^a conjugates under H, and if H'' is still another conjugate of H, it is one of p^b conjugates, and so on. Now H is not one of $1 + p^a + p^b + \cdots$ conjugates in G unless certain exponents $a, b, \cdots$, are zero. But if every permutation of H transforms H' into H', $\{H, H'\}$ is a subgroup of G because H' is not invariant in G.

CHAPTER II.

TRANSITIVE GROUPS.

§ 11.

Transitive Groups.—Homomorphic Groups.

Let G be a group of degree n in the letters $a_1, a_2, \cdots, a_n$; G is *transitive* if there is in G a permutation that replaces a_1 by a_i $(i = 2, 3, \cdots, n)$. If this condition is not fulfilled, G is *intransitive.*

I. If G is transitive the number of permutations of G that replace a_1 by a_i $(i = 2, 3, \cdots$, or $n)$, is equal to the number of permutations of G that fix a_1.

Let G_1 be the identity or the subgroup of G that does not displace the letter a_1. If the permutation S_i is $(a_1 a_i \cdots) \cdots$, all the permutations

$$G_1 S_i$$

are distinct and replace a_1 by a_i. If there is another permutation

$$T_i = (a_1 a_i \cdots) \cdots,$$

$G_1 S_i T_i^{-1}$ fixes a_1, so that

$$G_1 S_i T_i^{-1} = G_1$$

and

$$T_i = G_1 S_i .$$

II. The order of the subgroup that leaves fixed one letter of a transitive group of order g and degree n $(< g)$ is g/n.

III. An invariant subgroup of a transitive group displaces all the letters of the group.

In an intransitive group of degree n, the letters $a_1, a_2, \cdots$ displaced by it fall into sets such that no permutation of G replaces a letter of one set by a letter of another set, while some permutation of G replaces one letter of a set by any other letter of the set. If there are n_1 letters in the first set, n_2 in the second, $\cdots$, then

$$n = n_1 + n_2 + \cdots .$$

If the only permutation of G that leaves fixed the n_1 letters $a_1, a_2, \cdots, a_{n_1}$ is the identity, the erasure of the other $n - n_1$ letters of G leaves a transitive group on the letters $a_1, a_2, \cdots, a_{n_1}$ of the same order as

G. But when more than one permutation of G leaves fixed all the letters $a_1, a_2, \cdots, a_{n_1}$, the subgroup H they constitute is an invariant subgroup of G. To each permutation of the quotient group G/H there correspond therefore one or more permutations of a group on the letters $a_1, a_2, \cdots, a_{n_1}$. If two or more distinct permutations of the letters $a_1, a_2, \cdots, a_{n_1}$ correspond to one permutation of the quotient group, the product of either into the inverse of the other is in H, which is not possible if they are distinct permutations. The group (A) on the letters $a_1, a_2, \cdots, a_{n_1}$ is called a *transitive constituent,* or more accurately, a *transitive constituent group,* of the intransitive group, and the letters themselves are called a *set of transitivity* or a *transitive set.* To any group can be arbitrarily assigned as many transitive constituents in one letter as we like. Such constituents, while not groups, must occasionally be taken into account.

The order of A is equal to that of the quotient group G/H to which it is *isomorphic,* if by this term we mean that the permutations of the two groups are in a one-to-one relation such that the product of any two permutations in one group corresponds to the product (in the same order) of the two corresponding permutations of the other group. The groups G and G/H are said to be *multiply isomorphic* or to be in $(h, 1)$ *isomorphism.* This definition is applicable to two groups G and G' whenever G has a quotient group, with respect to an invariant subgroup of order h, to which G' is isomorphic; or it may be extended to the trivial case of any group G (of order g) and the identity, although the latter is not a group, between which obviously there always exists a $(g, 1)$ correspondence.

Let G of order g and G' of order g' have invariant subgroups H of order h and H' of order h', respectively. If between the permutations of G and G' a correspondence can be established so that G/H and G'/H' are isomorphic, then G is *(h, h') isomorphic,* or in an *(h, h') isomorphism,* to G'. This definition can also be extended if we replace H and H' by G and G', and the isomorphic quotient groups by the identity. Thus any two groups G and G' are (g, g') isomorphic. This trivial (g, g') isomorphism between G and G' is the relation that subsists when $\{G, G'\}$ is the direct product of G and G'.

These various sorts of correspondences may be described by one general term: *homomorphism.* Some correspondence can always be established between the permutations of any two groups, or between a group and the identity, or for that matter between two identical permutations, so that the two are *homomorphic.* Often this correspondence can be set up in several different ways.

When there is an $(h, 1)$ isomorphism between the intransitive group G and its transitive constituent A on the letters $a_1, a_2, \cdots, a_{n_1}$, it is not necessarily true that the constituent (B) in all the other letters of G is $(h, 1)$ isomorphic to A. In fact, if B and A are two (h, h') isomorphic groups on different sets of letters, and if we multiply the permutations of the corresponding divisions (g/hh' in number), the resulting intransitive group is of order g and has an invariant subgroup H of order h in letters of B, such that G/H is isomorphic to A. The simplest example of this sort of thing is presented by the group

$$\{(abc),\ (a'b'c'),\ (ab)(a'b')\}.$$

IV. The order of the subgroup of an intransitive group G of order g that leaves fixed one letter of a transitive constituent of degree n_1 $(< g)$ *is* g/n_1.

If g_1 is the order of the transitive constituent in question, and if H, of order h, as in the last paragraph, is the subgroup of G that fixes all the letters of that constituent, the order of the subgroup that fixes one letter is $hg_1/n_1 = g/n_1$.

§ 12.

Regular Groups and the Holomorph.

The quotient group G/H was defined in § 6 by a right-hand multiplication of the rows HS_i by permutations of G. Now

$$\begin{pmatrix} HS_i \\ HS_i^{-1} \end{pmatrix} \qquad (i=1,\ 2,\ \cdots,\ g/h),$$

is a permutation of order 2 of the letters of G/H. It transforms

$$\begin{pmatrix} HS_i \\ HS_iS_j \end{pmatrix}$$

into

$$\begin{pmatrix} HS_i^{-1} \\ HS_j^{-1}S_i^{-1} \end{pmatrix} = \begin{pmatrix} HS_k \\ HS_j^{-1}S_k \end{pmatrix} \qquad (k=1,\ 2,\ \cdots,\ g/h).$$

It is clear that two groups Γ and $t^{-1}\Gamma t$ are isomorphic, for if these permutations correspond: $t^{-1}at$ to a, and $t^{-1}bt$ to b; then $t^{-1}att^{-1}bt$ corresponds to ab. Hence a second group on the letters of G/H, isomorphic to G/H arises on left-hand multiplication of the rows of G with respect to H by permutations of G. Both groups are transitive and are *regular* groups, this term being used of a transitive group whose order is equal to its degree. In a regular group any permutation displaces either all the letters or none of them.

If

$$\begin{pmatrix} HS_i \\ HS_iS_j \end{pmatrix} = \begin{pmatrix} HS_i \\ HS_k^{-1}S_i \end{pmatrix} \quad (i=1\,,2\,,\cdots,\ g/h)\,,$$

by putting $S_i = S_1 = 1$,

$$HS_k^{-1} = HS_j\,,$$

and therefore

$$HS_iS_j = HS_jS_i\,.$$

Hence the cross-cut of G/H and of its transform by

$$\begin{pmatrix} HS_i \\ HS_i^{-1} \end{pmatrix}$$

is the central of each group. If the two groups are identical, G/H is Abelian, and conversely. Consider a permutation that is commutative with every permutation of G/H. It permutes the columns of the permutations of G/H (§ 1). If it fixes HS_1 (S_1 is the identity of G), it fixes all the letters of G/H. If it replaces HS_1 by HS_j, it replaces HS_1S_i by HS_jS_i $(i=1\,,2\,,\cdots,\ g/h)$; that is, it is the permutation

$$\begin{pmatrix} HS_i \\ HS_jS_i \end{pmatrix} \quad (i=1\,,2\,,\cdots,g/h)\,,$$

and is therefore in the transform of G/H by

$$\begin{pmatrix} HS_i \\ HS_i^{-1} \end{pmatrix}.$$

Let the identity be used in the place of H. Our quotient group G/H is now replaced by a regular group (Γ) isomorphic to G. Since the identity is in all groups, there is a regular group Γ of degree and order g isomorphic to every group G, and if G is not Abelian there is another regular group Γ', called the *conjoin* of Γ,

$$\Gamma' = \begin{pmatrix} HS_i \\ HS_i^{-1} \end{pmatrix} \Gamma \begin{pmatrix} HS_i \\ HS_i^{-1} \end{pmatrix}.$$

If G has k invariant permutations, the group

$$\{\Gamma\,,\ \Gamma'\}$$

is of order g^2/k. Since Γ' consists of all the permutations on these g letters that are commutative with each permutation of Γ, $\{\Gamma\,,\ \Gamma'\}$ is the largest group in the letters of Γ which transforms the permutations of Γ according to its own permutations. That is, all other permutations that transform Γ into itself put Γ in an isomorphism with itself in a way that can not be brought about by any permutation of Γ. To fix this distinction we call these one-to-one correspondences of Γ to itself *inner* and *outer isomorphisms,* respectively. The subgroup of $\{\Gamma, \Gamma'\}$ that leaves S_1 fixed is of order g/k and gives all the distinct inner isomorphisms of Γ to itself. It should be noticed that this group of inner isomorphisms of Γ is isomorphic to the central quotient group G/K, or to G when G has no central. In many important groups there is no central and Γ has no outer isomorphisms. Such groups are called *complete* groups.

But if outer isomorphisms for Γ exist, they fix S_1, transform Γ', as well as Γ, into itself, and therefore transform the group of inner isomorphisms into itself. Then if we are able to form the largest group of degree g in which Γ is invariant, it may be called the *holomorph* of Γ (or of G), and in it the subgroup that leaves one letter fixed is I, the *group of isomorphisms* of G. No two permutations of I transform the permutations of Γ in exactly the same way. The group of inner isomorphisms, when it does not coincide with I, is an invariant subgroup of I.

In § 3 all the permutations that transform a cyclical group of degree and order p into itself were found. They constitute the holomorph of the group of order p. This group is of order $p(p-1)$ and is called the *metacyclic* group. When $p=3$, it is

$$\{(a_1a_2a_3),\ (a_1a_2)\}.$$

When $p=5$, it is

$$\{(a_1a_2a_3a_4a_5),\ (a_2a_3a_5a_4)\},$$

of order 20. The subgroup of order $p-1$ is the group of isomorphisms of the cyclic group of order p. The latter, being Abelian, has no inner isomorphisms. It is worthy of remark that when the cyclic group of order p is given, all the other permutations of the metacyclic group are completely determined. Obviously this is true of any holomorph, once the group Γ is fully given. The metacyclic group has an invariant subgroup of order $p\delta$ corresponding to every divisor δ of $p-1$. One of these subgroups is the diedral group of order $2p$.

§ 13.

Complete Groups.

Complete groups were defined in the preceding section. The reason for this name may be found in the principal theorem concerning them:

I. A group, of which a complete group H is an invariant subgroup, is the direct product of H and another group.

The given group G may be written in the array:

$$HS_i \qquad (i = 1, 2, \cdots, g/h).$$

Let $\sigma_1, \sigma_2, \cdots, \sigma_h$ be the permutations of H. Since H admits no outer isomorphisms a permutation of $\sigma_i S_j$ permutes every permutation of H exactly as does some permutation σ_k of H. Now $\sigma_k^{-1}\sigma_i S_j$ $(S_j \neq 1)$ is not the identity, and therefore the permutations $S_1, S_2, \cdots$ may be so taken that every permutation of the group

$$K = \{S_1, S_2, \cdots, S_{g/h}\}$$

is commutative with every permutation of H. But the identity is the only invariant permutation of H, so that K is of order g/h. Then G is a direct product (§ 8).

Some useful information about groups of isomorphisms can be obtained from the following theorem. It will in particular enable us to show (§ 54) that the symmetric group on n letters $(n \neq 2; n \neq 6)$ is a complete group.

II. If $S_1, S_2, \cdots, S_n$ are the permutations of the group G which transform into itself each of certain permutations (groups, functions)

$$\Sigma_1, \Sigma_2, \cdots, \Sigma_m,$$

constituting a complete set of conjugates under the holomorph of G, then the outer isomorphisms of G which also transform Σ_i into Σ_i $(i = 1, 2, \cdots, m)$ transform any permutation of G into itself multiplied by one of the permutations $S_1, S_2, \cdots, S_n$.

If $n = g$, the order of G, the theorem is obviously true.

If $g > n \geqq 2$, the permutations $S_1, S_2, \cdots, S_n$ constitute an invariant subgroup (E) of K, the holomorph of G. If $n = 1$, E represents the identity of G. Consider T, a permutation of the group of isomorphisms of G that also transforms Σ_i into Σ_i $(i = 1, 2, \cdots, m)$. The powers of T which are in G are by hypothesis in E. Let I_i be the largest subgroup of G under which Σ_i is invariant. Then $\{T, I_i\}$ is the largest subgroup of $\{G, T\}$ under which Σ_i is invariant. The groups $\{T, I_i\}$ are conjugate under K. The permutations of E, and no others, are common to $I_1, I_2, \cdots, I_m$. Then the group $\{T, E\}$ is transformed into itself by all the permutations of $\{T, G\}$. If E is the identity, $\{T, G\}$ is therefore the direct product of $\{T\}$ and G, and T is not an outer isomorphism, but the identity. If $n \geqq 2$, $\{T, G\}/E$ is the direct product of $\{T, E\}/E$ and G/E (§ 8, IV). This is equivalent to saying that T transforms any permutation of G into itself multiplied by some permutation of E, and the theorem is proved.

Let S and S_1 be two permutations of the group of isomorphisms of G, and let it be assumed that E of the above theorem is the identity. Now

$$\begin{pmatrix} \Sigma_i \\ S^{-1}\Sigma_i S \end{pmatrix}\begin{pmatrix} \Sigma_i \\ S_1^{-1}\Sigma_i S_1 \end{pmatrix} = \begin{pmatrix} \Sigma_i \\ S_1^{-1}S^{-1}\Sigma_i SS_1 \end{pmatrix}$$

$$= \begin{pmatrix} \Sigma_i \\ (SS_1)^{-1}\Sigma_i SS_1 \end{pmatrix} \qquad (i = 1, 2, \cdots, m),$$

so that the permutations of the letters Σ_i which arise by transforming Σ_i $(i = 1, 2, \cdots, m)$ by the permutations of the group of isomorphisms of G constitute a group isomorphic to the group of isomorphisms of G. Hence:

III. If the identity is the only permutation of a group G which transforms into itself each of the permutations (groups, functions)

$$\Sigma_1, \Sigma_2, \cdots, \Sigma_m,$$

forming a complete set of conjugates under the holomorph of G, then the permutations of the letters

$$\Sigma_1, \Sigma_2, \cdots, \Sigma_m,$$

when the m conjugates are transformed by all the permutations of the group of isomorphisms of G, constitute a transitive group isomorphic to that group of isomorphisms.

If two permutations (groups, functions) Σ and Σ_1 are conjugate under the holomorph of G, but are not conjugate under G, it is easy to see that the number of conjugates (under G) of Σ is the same as the number of conjugates of Σ_1. For if S is a permutation of G, and if T, an outer isomorphism, transforms Σ into Σ_1, and S into S_1, then T transforms $S^{-1}\Sigma S$ into $S_1^{-1}\Sigma_1 S_1$. Hence:

IV. The number of conjugates under G of any permutation (group, function) divides the number of its conjugates under the holomorph of G.

In the metacyclic group there are p conjugate subgroups of order $p - 1$ and no other subgroup of this order. No one of the subgroups of order $p - 1$ is transformed into itself by a permutation not in it. Then the group of isomorphisms of the metacyclic group is isomorphic to a transitive group of degree p. Since the metacyclic group is already the holomorph of the cyclic group of order p, it is a complete group. Hence the theorem:

V. The metacyclic group is a complete group.

The symmetric group of degree 4 has four cyclic subgroups of order 3 generated by

$$(abc), \quad (abd), \quad (acd), \text{ and } (bcd).$$

No permutation (except the identity) transforms each of these subgroups into itself. Then the group of isomorphisms of the symmetric group of degree 4 is isomorphic to a transitive group of degree 4. In other words the symmetric group of degree 4 is a complete group.

This likewise proves that the group of isomorphisms of the alternating group of degree 4 is isomorphic to the symmetric group of degree 4.

§ 14.

Transitive Groups Isomorphic to a Given Group.

Let the subgroup H of § 6 be freed from the restriction that it is invariant in G. Assume in addition that H contains no invariant subgroup of G. Let $\sigma_1, \sigma_2, \cdots, \sigma_h$ be the permutations of H, and let $S_2, S_3, \cdots$ be permutations of G not in H so chosen that G may be written in the array $(S_1 = 1)$

$$HS_1, HS_2, HS_3, \cdots, HS_{g/h}.$$

Now when all the permutations of this array are multiplied (on the right) by the permutations of H, the g/h rows of G are permuted thus:

$$\begin{array}{l}
HS_1\sigma_1, HS_2\sigma_1, HS_3\sigma_1, \cdots, HS_{g/h}\sigma_1, \\
HS_1\sigma_2, HS_2\sigma_2, HS_3\sigma_2, \cdots, HS_{g/h}\sigma_2, \\
\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
HS_1\sigma_i, HS_2\sigma_i, HS_3\sigma_i, \cdots, HS_{g/h}\sigma_i, \\
\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
HS_1\sigma_h, HS_2\sigma_h, HS_3\sigma_h, \cdots, HS_{g/h}\sigma_h.
\end{array}$$

We may write these permutations:

$$\begin{pmatrix} HS_i \\ HS_i\sigma_j \end{pmatrix} \qquad (i = 1, 2, \cdots, g/h).$$

They fix HS_1. If one of them fixes all the letters,

$$\sigma_x S_i = \sigma_y S_i \sigma_j \qquad (i = 2, 3, \cdots, g/h),$$

$$S_i \sigma_j S_i^{-1} = \sigma_y^{-1} \sigma_x,$$

and H contains all the conjugates under G of σ_j, that is, contains one of the invariant subgroups of G, contrary to hypothesis. These h permutations constitute a group isomorphic to H. For

$$\begin{pmatrix} HS_i \\ HS_i\sigma_j \end{pmatrix}\begin{pmatrix} HS_i \\ HS_i\sigma_k \end{pmatrix} = \begin{pmatrix} HS_i \\ HS_i\sigma_j\sigma_k \end{pmatrix}.$$

Now multiply the original array by all the other permutations of G:

$$\begin{array}{lllll} HS_1S_2\,, & HS_2^2\,, & HS_3S_2\,, & \cdots, & HS_{g/h}S_2\,, \\ HS_1\sigma_2S_2\,, & HS_2\sigma_2S_2\,, & HS_3\sigma_2S_2\,, & \cdots, & HS_{g/h}\sigma_2S_2\,, \\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot \\ HS_1\sigma_iS_j\,, & HS_2\sigma_iS_j\,, & HS_3\sigma_iS_j\,, & \cdots, & HS_{g/h}\sigma_iS_j\,, \\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot \end{array}$$

Since we have

$$\begin{pmatrix} HS_i \\ HS_i\sigma_jS_k \end{pmatrix}\begin{pmatrix} HS_i \\ HS_i\sigma_uS_v \end{pmatrix} = \begin{pmatrix} HS_i \\ HS_i\sigma_jS_k\sigma_uS_v \end{pmatrix},$$

the permutations in the letters HS_1, HS_2, $\cdots$ constitute a transitive group of degree g/h and order g, isomorphic to G. Hence, combining this result with IV of § 11, we have:

I. The necessary and sufficient condition that a group G be isomorphic to some transitive group of degree n is that it have a subgroup of index n which includes no invariant subgroup of G.

§ 15.

A Group Isomorphic to the Symmetric Group.

This last theorem can be well illustrated by one of the transitive groups isomorphic to the symmetric group of degree n $(\geqq 4)$. The largest intransitive subgroup of the symmetric group is the direct product of the symmetric group of degree $n-2$ and a group of degree and order 2 in the two other letters. Suppose this intransitive group of order $2(n-2)!$ to include a subgroup invariant in the symmetric group. Let $1, (n-1, n)$ be its transitive constituent of degree 2. Since an invariant subgroup of a transitive group displaces all the letters of the group, our invariant subgroup must have the transitive constituent $\{(n-1\,, n)\}$. The permutation $(1\,, n)$ must transform it into itself, and therefore $\{(1\,, n-1)\}$ is also a transitive constituent, which is absurd. Since, then, this subgroup includes no invariant subgroup invariant in the symmetric group, the latter is isomorphic to a transitive group of degree $n\ (n-1)/2$. There are just as many of these intransitive subgroups of order $2(n-2)!$ as there are transpositions of n letters, so that the permutations of the required transitive group of degree $n(n-1)/2$ record the permutations of the transpositions

$$(23)\,,\ (31)\,,\ (12)\,,\ (14)\,,\ (24)\,,\ (34)\,,\ (15)\,,\ (25)\,,\ (35)\,,\ (45)\,,$$
$$\cdot\ \cdot\ \cdot\ \cdot,\ \ (1n)\,,\ (2n)\,,\ \cdots,\ (n-1\,, n)\,,$$

by the symmetric group on the subscripts $1, 2, \cdots, n$. Let us write for these transpositions the letters

$$b_1, b_2, b_3, a_1, a_2, a_3, c_1, c_2, c_3, c_4, \cdots, l_1, l_2, \cdots, l_{n-1}.$$

Then to the generators of the symmetric group,

$$(12), (13), (14), (45), (46), (47), \cdots, (4n),$$

correspond in order

$$\begin{aligned}
S &= (a_1a_2)(b_1b_2)(c_1c_2)(d_1d_2)(e_1e_2) \cdots (l_1l_2), \\
S_1 &= (a_1a_3)(b_1b_3)(c_1c_3)(d_1d_3)(e_1e_3) \cdots (l_1l_3), \\
S_2 &= (a_2b_3)(a_3b_2)(c_1c_4)(d_1d_4)(e_1e_4) \cdots (l_1l_4), \\
S_3 &= (a_1c_1)(a_2c_2)(a_3c_3)(d_4d_5)(e_4e_5) \cdots (l_4l_5), \\
S_4 &= (a_1d_1)(a_2d_2)(a_3d_3)(c_4d_5)(e_4e_6) \cdots (l_4l_6), \\
S_5 &= (a_1e_1)(a_2e_2)(a_3e_3)(c_4e_5)(d_4e_6) \cdots (l_4l_7), \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
S_{n-2} &= (a_1l_1)(a_2l_2)(a_3l_3)(c_4l_5)(d_4l_6) \cdots (k_4l_{n-1}).
\end{aligned}$$

To $(n-1, n)$ corresponds

$$R = (k_1l_1)(k_2l_2) \cdots (k_{n-2}l_{n-2}),$$

which, with

$$\{S, S_1, S_2, \cdots, S_{n-4}\},$$

generates the subgroup that leaves l_{n-1} fixed. This subgroup

$$\{S, S_1, S_2, \cdots, S_{n-4}\},$$

has two symmetric constituents of degree $n-2$ in the letters $k_1, k_2, \cdots, k_{n-2}$ and $l_1, l_2, \cdots, l_{n-2}$, respectively, and one transitive constituent of degree $(n-2)(n-3)/2$ isomorphic to the symmetric group of degree $n-2$. Then the subgroup that leaves one letter fixed has just two transitive constituents, one of order $2(n-2)!$ and one of order $(n-2)!$.

Certainly no permutation of the symmetric group can permute fewer transpositions than does the transposition (12), which permutes just $2n-4$ transpositions.

§ 16.

Definition of Primitive and Imprimitive Groups, of Equivalent and Similar Groups.

A transitive group of degree n is *imprimitive* if there are n/m systems of m $(1 < m < n)$ letters, with no letter in common, that are permuted as units by the group. The systems are known as *systems of imprimitivity* of the group.

If a transitive group has no such systems of imprimitivity it is called a *primitive* group. This definition may be put in positive form by saying that some permutation of a *primitive* group of degree n replaces one letter of any alleged system of m $(1 < m < n)$ letters by a letter of that system, and one of the m letters by a letter not a member of the system.

Groups of prime degree are primitive if they are transitive. Cyclic groups generated by a circular permutation of composite order are imprimitive. Thus the systems of imprimitivity of

$$1,\quad (ab\alpha\beta)\,,\quad (a\alpha)(b\beta)\,,\quad (a\beta\alpha b)$$

are a , α and b , β . When writing the letters of systems of imprimitivity of a transitive group we shall in the future omit the commas. Systems of imprimitivity of the regular group of order 6, isomorphic to the symmetric group of order 6:

$$1,(123)(465),(132)(456),(14)(25)(36),(15)(26)(34),(16)(24)(35)\,;$$

are 123 and 456. Three of the permutations transform each system into itself. Other systems are 14 , 26 , 35 . If these three systems are tagged S_1 , S_2 , S_3 , respectively, the group is isomorphic to

$$1\,,\quad (S_1S_2S_3)\,,\quad (S_1S_3S_2)\,,\quad (S_2S_3)\,,\quad (S_1S_3)\,,\quad (S_1S_2)\,.$$

In like manner 15 , 24 , 36 and 16 , 25 , 34 are systems of imprimitivity and they too are permuted according to the above group.

If a group G has a subgroup H , the regular group Γ isomorphic to G is imprimitive. For the rows

$$HS_i \qquad (i = 1\,, 2\,, \cdots, \; g/h)\,,$$

are permuted as units, and one system of imprimitivity is

$$\sigma_1\,,\ \sigma_2\,,\ \cdots\cdots,\ \sigma_h\,,$$

if these are the permutations of H , treated as letters of Γ . Exactly the same regular group Γ is obtained from all groups isomorphic to Γ (that is, to G). It follows that all those subgroups of index n in Γ , which include no invariant subgroup of G , and which are conjugate in the holomorph of Γ , give the same transitive group of degree n isomorphic to Γ .

We say that two groups are *equivalent* when there exists a permutation by which one can be transformed into the other. If no such permutation exists the two groups are *non-equivalent,* or *distinct.* But when the word *distinct* is applied to subgroups of some group, it merely means that the two subgroups under discussion are not in every respect identical. Thus

$$1\,,\ (ab)\ ;\ \text{and}\ 1\,,\ (ac)\ ;$$

are not distinct groups but are distinct subgroups of the symmetric group of degree $n\,(>2)$, in which they are conjugate.

Two equivalent groups G and G' are *similar* (cf. § 3) when, if S_i and S'_i are corresponding permutations in some isomorphism of G to G', given in advance, a permutation T exists such that

$$T^{-1}S_iT = S'_i \qquad (i = 1\,,\ 2\,,\ \cdots,\ g)\,.$$

If no such permutation T exists, then G and G' are *dissimilar.*

To illustrate the distinction between equivalence and similarity, the groups

$$1\,,\ (ab)\,,\ (cd)\,,\ (ab)(cd)\,,$$

and

$$1\,,\ (\alpha\beta)\,,\ (\alpha\beta)(\gamma\delta)\,,\ (\gamma\delta)$$

are equivalent, because $(a\alpha)(b\beta)(c\gamma)(d\delta)$ transforms one into the other. The order in which the permutations are written exhibits an isomorphism between the two groups. But with respect to this isomorphism the groups are dissimilar, for the two corresponding permutations (cd) and $(\alpha\beta)(\gamma\delta)$ are not similar. It must be emphasized that when two groups are similar, the underlying isomorphism cannot in general be disturbed without turning them into dissimilar groups. Two groups whose permutations are identical are equivalent, but not always similar. For example, if (ab) corresponds to (ab), and (cd) corresponds to $(ab)(cd)$, the groups $\{(ab)\,,\ (cd)\}$ and $\{(ab)\,,\ (ab)(cd)\}$ are dissimilar.

If two transitive groups G and G' are equivalent the permutation T which transforms G into G' can be chosen so that it transforms a given subgroup that leaves one letter of G fixed into any subgroup of G' that leaves one letter of G' fixed. Hence:

I. There are as many distinct transitive groups of degree n isomorphic to a given group G as there are in Γ (the regular group isomorphic to G) complete sets of subgroups of index n, conjugate under the holomorph of G, which include no invariant subgroup of G.

One of the easiest applications of this theorem is to the diedral groups. In the holomorph of a diedral group of order $2n$ $(n > 2)$, the n permutations of order 2 which transform the permutation of order n into its inverse form a single conjugate set. Furthermore the only subgroup of the diedral group which includes no invariant subgroup of the entire group is of order 2 and is one of the n subgroups of order 2 whose generators transform the permutation of order n into its inverse. Therefore there are only two distinct transitive groups isomorphic to a diedral group of order $2n$. One is the regular group and the other is of degree n.

§ 17.

The Subgroup That Fixes One Letter of a Transitive Group.

Consideration of the regular group Γ isomorphic to G shows that if G is a transitive group on the letters $a_1, a_2, \cdots, a_n$ it will be imprimitive if the subgroup H of order h (> 1) that fixes a_1 is a subgroup of another subgroup H' of G. Then if H is a *maximal* subgroup of G, that is, is not a subgroup of a subgroup of G, G is primitive. When H fixes a_i in addition to a_1, and is not the identity, all permutations of G that replace a_1 by a_i transform H into itself. Conversely, if

$$S = (a_1 a_i \cdots) \cdots$$

transforms H into itself, the h permutations HS do so, and therefore H fixes a_i. In consequence:

I. If H is invariant in a subgroup of G of order αh $(\alpha > 1)$, H fixes exactly α letters of G, and conversely.

If H is not an invariant subgroup of a subgroup of G, H displaces $n - 1$ letters. In particular, if G is primitive, H is of degree $n - 1$.

A property of the symmetric group of degree n is that one of its permutations replaces any $n - 1$ letters by any $n - 1$ arbitrarily chosen letters. When in a group G a permutation exists that replaces any t $(\geqq 2)$ letters by any t arbitrarily chosen letters, G is said to be *multiply transitive*, or more exactly, *t-ply transitive* or *t times transitive*. The symmetric group is $(n - 1)$-ply transitive. A multiply transitive group is a fortiori primitive. The subgroup of a *t-ply* $(t \geqq 2)$ transitive group G that leaves fixed one, two, $\cdots$, $t - 1$ letters is transitive, and the order of G is

$$n\,(n - 1) \cdots (n - t + 1)\, m,$$

where m is the order of the subgroup of G that leaves t letters fixed. If the subgroup H of G that leaves one letter a_1 fixed is a transitive group of degree $n - 1$, then G is at least doubly (2-ply) transitive. Since, when G is multiply transitive, H is transitive of degree $n - 1$, the cross-cut of $S^{-1}HS$ (S replaces a_1 by a_i) and H is of order $h/(n - 1)$, or reduces to the identity. Consequently (see § 8, II) the number of distinct permutations in HSH is $h(n - 1)$, that is, the array HSH includes all the permutations of G not in H. This, then, is a necessary condition that the transitive group H of degree $n - 1$ is the subgroup that fixes one letter of a multiply transitive group of degree n. That it is also a sufficient condition follows from the fact that all the permutations HSH displace a_1, the letter fixed by H, if S displaces a_1, so that H is actually a maximal subgroup of G. We have proved:

II. The necessary and sufficient conditions that a group G be isomorphic to a multiply transitive group of degree n are:

(1) G has a subgroup H of index n which includes no invariant subgroup of G.

(2) Any permutation of G is in H or in HSH, where S is any permutation of G not in H.

§ 18.

An Existence Theorem for Multiply Transitive Groups.

When a group H of degree $n-1$ and order h is given it is possible to set up a large number of permutations S that generate with H a transitive group of degree n. It is of importance to know what conditions S must satisfy in order that $\{H, S\}$ may be of order nh. It is a difficult question to answer when H is intransitive. But when H is a non-regular transitive group, and especially when H is doubly transitive, the following theorem gives the required conditions in convenient form.

I. Let H be a transitive, non-regular group of degree $n-1$ and of order h. Let all the permutations of H occur in the arrays F, FRF, FR_1F, $\cdots$, FR_kF, where F is the subgroup that leaves one letter of H fixed, and R, R_1, $\cdots$ are permutations of H not in F. If S is a permutation of order 2 which displaces one letter new to H, and such that

$$SFS = F\,,\ SRS = HSH\,,\ SR_1S = HSH\,,\ \cdots,\ SR_kS = HSH\,,$$

then $\{H, S\}$ is of order nh.

Every permutation of $G = \{H, S\}$ can be written in the form of a finite continued product

$$\cdots HSHSH \cdots,$$

and this product can be reduced to H or to HSH if

$$SHS = H\,,$$

or if

$$SHS = HSH\,.$$

The necessary and sufficient condition that $SFRFS$ $(=FSRSF)$ reduces to HSH is that

$$SRS = HSH\,.$$

Since every permutation of the array HSH displaces a letter new to H if S does so, H is seen to be a maximal subgroup of G.

The following discussion will be found helpful when we come to apply this theorem to actual groups.

If H is doubly transitive F and FRF include all the permutations of H. If a is a letter of F and b is the letter of H that F leaves fixed, some permutation of order 2 of H can be transformed into $(ab)\cdots$, and this permutation may be called R. Since G is triply transitive, and H is a maximal subgroup of G, a permutation $(bc)(a)\cdots$ of order 2, in which c is new to H, may be used for S. Then the condition

$$SRS=HSH\,,$$

since $RS=(acb)\cdots$, reduces to

$$(RS)^3=F\,.$$

If H is not doubly transitive, F leaves b fixed, and has two or more other transitive constituents (counting those of one letter). Let us select one letter from each of these $k+1$ transitive sets: a, a_1, $\cdots$, a_k. If now

$$\begin{aligned} R&=(ba\cdots)\cdots,\\ R_1&=(ba_1\cdots)\cdots,\\ &\cdots\cdots\cdots\\ R_k&=(ba_k\cdots)\cdots \end{aligned}$$

are permutations of H, all the permutations of H can be written in the arrays

$$F\,,\;FRF\,,\;FR_1F\,,\;\cdots,\;FR_kF\,.$$

For FRF, say, includes all the permutations of H which replace b by a letter of the transitive set a, a', $\cdots$ of F. Now let $S=(bc)\cdots$ be a permutation of order 2 (there certainly is one such in G) that generates with the maximal subgroup H the doubly transitive group G. It may be that some of the permutations R, R_1, $\cdots$ can be so chosen that

$$(R_iS)^3=F \qquad (i=0\,,1\,,\cdots,\text{ or }k\,;\,R_0=R)\,.$$

But this is not always possible. In general we have to find two permutations U and V in H that will satisfy the equation

$$SR_iS=USV\,.$$

Now

$$R_i=(ba_i\cdots)(c)\cdots.$$

Let S replace a_i by the letter a_j' of the set a_j, a_j', $\cdots$ of F. Then

$$SR_iS=(b)(ca_j'\cdots)\cdots,$$

so that

$$V = (c)(ba'_j \cdots) \cdots$$

$$= R_j T^{-1},$$

where T is a permutation of F which replaces a'_j by a_j. The permutation

$$U = SR_iSTR_j^{-1}S$$

or, if we prefer it,

$$T^{-1}UT = (ST)^{-1}R_i(ST)R_j^{-1}(ST),$$

for some

$$T = (a'_j a_j \cdots) \cdots$$

of F, should be in H. If U proves to be a permutation R_kT_1, where T_1 belongs to F, we have not only

$$SR_iS = HSH,$$

but also

$$SR_jS = HSH,$$

and

$$SR_kS = HSH.$$

§ 19.

The Average Number of Letters in the Permutations of a Transitive Group.

The characteristic (§ 2) of a permutation of a group of degree n is the difference between the degree of the group and the degree of the permutation. The characteristic of the identity is n.

Let G be a transitive group of order g and degree n, and let the permutations of G lie in complete sets of conjugates of $g_1, g_2, \cdots, g_h$ permutations each. Let the subgroup (G') of G that leaves one letter fixed include just g'_i permutations of the i^{th} conjugate set of G. Now conjugate permutations have equal characteristics (§ 2). Let χ_i be the characteristic of any permutation of the i^{th} conjugate set of G, that one, say, in which there are g_i members. Consider a permutation of G'. It has g'_i conjugates in G' under G and fixes χ_i letters of G. Therefore

$$g_i = ng'_i/\chi_i,$$

and

$$\sum_{i=1}^{h} g_i\chi_i = \sum_{i=1}^{h} ng'_i = n\sum_{i=1}^{h} g'_i = n \cdot g/n$$

$$= g.$$

That is, the sum of the characteristics of all the permutations of a transitive group is equal to the order of the group, or in other words:

I. The average number of letters in the permutations of a transitive group of degree n is $n-1$.

If G is an intransitive group, in which there are α transitive constituents (even if we count those of one letter)

$$\sum_{i=1}^{h} g_i\chi_i = \alpha g .$$

Hence:

II. The average number of letters in the permutations of an intransitive group, in which there are α transitive constituents, is $n-\alpha$.

The identity leaves fixed n letters of a transitive group of degree n, and therefore, by Theorem I:

III. A transitive group of degree n contains at least $n-1$ permutations which displace n letters.

CHAPTER III.

GROUP CHARACTERISTICS.

§ 20.

The Normal Form.

Let the substitution

$$A : \qquad x_i = \sum_{j=1}^{n} a_{ij}x'_j \qquad (i=1, 2, \cdots, n)$$

transform the linear function

$$\sum_{i=1}^{n} e_{1i}x_i ,$$

where not every e_{1i} is zero, into

$$\lambda \sum_{i=1}^{n} e_{1i}x'_i .$$

Since

$$\sum_{i=1}^{n} e_{1i}x_i = \sum_{i=1}^{n} e_{1i} \sum_{j=1}^{n} a_{ij}x'_j = \sum_{j=1}^{n} \sum_{i=1}^{n} e_{1i}a_{ij}x'_j = \lambda \sum_{j=1}^{n} e_{1j}x' ,$$

we have

$$(1) \qquad \sum_{i=1}^{n} e_{1i}a_{ij} = \lambda e_{1j} \qquad (j=1, 2, \cdots, n) .$$

Then λ must be a root of the equation

$$(2) \qquad \begin{vmatrix} a_{11}-t & a_{12} & a_{13} & \cdot & \cdot & \cdot & a_{1n} \\ a_{21} & a_{22}-t & a_{23} & \cdot & \cdot & \cdot & a_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & a_{n3} & & & & a_{nn}-t \end{vmatrix} = 0 .$$

This equation is known as the *characteristic equation* of the substitution A. Since the left-hand member of (2) is the determinant (§ 2) of a substitution whose coefficients are the elements of the determinant, t being arbitrary, it may be remarked in passing that:

I. The characteristic equation of A is invariant under transformation of A by any substitution of non-zero determinant.

When a root λ of the equation (2) has been found and put in (1), equations (1) may be solved for the ratios of the quantities e_{11}, e_{12}, $\cdots$,

e_{1n}. Suppose a set of solutions for e_{1i} has been obtained, corresponding to $t = \lambda_1$. The substitution

$$T_1: \qquad y_i = \sum_{j=1}^{n} e_{ij} x_j \qquad (i = 1, 2, \cdots, n),$$

in which some e_{1j} is not zero while $n^2 - n$ coefficients are arbitrary, and whose determinant may therefore be made different from zero, transforms A into a substitution

$$\begin{aligned} y_1 &= \lambda_1 y'_1, \\ y_i &= \sum_{j=1}^{n} b_{ij} y'_j \qquad (i = 2, 3, \cdots, n). \end{aligned}$$

Now consider the substitution

$$B: \qquad y_i = \sum_{j=2}^{n} b_{ij} y'_j \qquad (i = 2, 3, \cdots, n).$$

Its characteristic equation is the quotient of (2) by $t - \lambda_1$. Set up the substitution

$$z_i = \sum_{j=2}^{n} f_{ij} y_j \qquad (i = 2, 3, \cdots, n),$$

in which the f_{2j} are solutions of the $n - 1$ equations

$$\sum_{i=2}^{n} f_{2i} b_{ij} = \lambda_2 f_{2j} \qquad (j = 2, 3, \cdots, n),$$

and λ_2 is a solution of the characteristic equation of B; the arbitrary coefficients are so taken that the determinant of the substitution is not zero. This substitution transforms B into

$$\begin{aligned} z_2 &= \lambda_2 z'_2, \\ z_i &= \sum_{j=2}^{n} c_{ij} z'_j \qquad (i = 3, 4, \cdots, n). \end{aligned}$$

Then the substitution

$$T_2: \qquad \begin{aligned} z_1 &= y_1, \\ z_i &= \sum_{j=2}^{n} f_{ij} y_j \qquad (i = 2, 3, \cdots, n) \end{aligned}$$

is of non-zero determinant and the product $T_1 T_2$ transforms A into

$$\begin{aligned} z_1 &= \lambda_1 z'_1, \\ z_2 &= c_{21} z'_1 + \lambda_2 z'_2, \\ z_i &= \sum_{j=1}^{n} c_{ij} z'_j \qquad (i = 3, 4, \cdots, n). \end{aligned}$$

This process may be continued until A is transformed into a substitution in which all the coefficients above the principal diagonal are zero and the coefficients of the principal diagonal are the roots of the characteristic equation A in any desired order:

$$L: \qquad x_i = \sum_{j=1}^{i} \lambda_{ij} x'_j \qquad (i=1, 2, \cdots, n) .$$

A substitution in which all the coefficients above the principal diagonal are zero is in *normal* form or is a *normal substitution.* Hence the last result may be stated:

II. Any substitution can be transformed into the normal form.

It should be noticed that the product of two normal substitutions is a normal substitution.

The coefficients in the principal diagonal of a normal substitution are called the *multipliers* of the substitution. If the only non-zero coefficients of a substitution are in the principal diagonal, the substitution is said to be a *multiplication.*

The *variety* of a substitution is the number of distinct roots in its characteristic equation. If a multiplication is of variety one, it is known as a *similarity substitution:*

$$x_i = \lambda x'_i \qquad (i=1, 2, \cdots, n) .$$

Such a substitution is commutative with every substitution on the same n variables.

§ 21.

The Open Product.

A substitution on n variables, that replaces s $(< n)$ of its variables by linear functions of themselves and replaces the $n - s$ other variables also by linear functions of themselves, is called an *open product,* and the two substitutions on the s and $n - s$ variables are called *components* of the open product. Of course a component may likewise be an open product.

The substitution

$$\begin{aligned} x_1 &= a x'_1 + b x'_2 . \\ x_2 &= c x'_1 + d x'_2 , \\ x_3 &= e x'_3 , \end{aligned}$$

is an example of an open product. It is the product of the commutative substitutions

$$x_1 = ax'_1 + bx'_2 \, ,$$
$$x_2 = cx'_1 + dx'_2 \, .$$
$$x_3 = x'_3 \, ,$$

and

$$x_1 = x'_1 \, .$$
$$x_2 = x'_2 \, ,$$
$$x_3 = ex'_3 \, .$$

If $\lambda_{ss} \neq \lambda_{tt}$ $(s > t)$ we may transform L (of § 20) by the substitution

$$T_{st} : \quad \begin{aligned} y_i &= x_i && (i = 1, 2, \cdots, s-1) \, , \\ y_s &= h_{st} x_t + x_s \, , && \\ y_i &= x_i && (i = s+1, s+2, \cdots, n) \, . \end{aligned}$$

The transform $T_{st}^{-1} L T_{st}$ does not differ from L in the first $s - 1$ lines. All its coefficients above the principal diagonal are zero. The s^{th} and following equations of the transformed substitution are

$$y_s = \sum_{j=1}^{t} (\lambda_{sj} + h_{st}\lambda_{tj}) y'_j - h_{st}\lambda_{ss} y'_t + \sum_{j=t+1}^{s} \lambda_{sj} y'_j \, ,$$
$$y_i = \sum_{j=1}^{i} \lambda_{ij} y'_j - h_{st}\lambda_{is} y'_t \qquad (i = s+1, s+2, \cdots, n) \, .$$

Only the coefficients of the first t columns of $T_{st}^{-1} L T_{st}$ differ from the corresponding coefficients of L. If we put

$$h_{st} = \lambda_{st} / (\lambda_{ss} - \lambda_{tt}) \, ,$$

a zero appears in $T_{st}^{-1} L T_{st}$ where λ_{st} stood in L. By a previous transformation the various equal multipliers of A have been grouped together along the principal diagonal of L, let us say. Hence if λ_{ss} is the first coefficient of the principal diagonal different from λ_{11}, we replace $\lambda_{s,\,s-1}$, $\lambda_{s,\,s-2}$, $\cdots$, λ_{s1}, in turn by zero, then treat the next row in the same way, and so on. In this way all the coefficients below and on a line with unequal elements of the principal diagonal of L can be removed. The final transform, if A has k unequal multipliers each repeated n_i $(i = 1, 2, \cdots, k)$ times, consists of k substitutions on n_i variables no two of which have a variable in common. We have proved:

I. Any substitution of variety $\geqq 2$ *can be transformed into an open product of component normal substitutions of variety one.*

§ 22.

The Canonical Substitution.

I. The normal substitution of variety one

$$M: \qquad x_i = \sum_{j=1}^{i} \mu_{ij} x'_j \qquad (\mu_{11} = \lambda; i = 1, 2, \cdots, n)$$

can be transformed into

$$C: \quad \begin{aligned} x_1 &= \lambda x'_1, \\ x_i &= \varepsilon_i x'_{i-1} + \lambda x'_i \quad (\varepsilon_i = 0 \text{ or } 1;\ i = 2, \cdots, n). \end{aligned}$$

Let this theorem be assumed true for any two substitutions M and C on not more than $n-1$ variables. If $n = 1$, M is already in the required form, as it is also if $n = 2$ and $\mu_{21} = 0$. If $n = 2$ and $\mu_{21} \neq 0$, M is transformed into

$$\begin{aligned} y_1 &= \lambda y'_1, \\ y_2 &= y'_1 + \lambda y'_2, \end{aligned}$$

by the substitution

$$\begin{aligned} x_1 &= y_1, \\ x_2 &= \mu_{21} y_2. \end{aligned}$$

Let

$$M_{n-1}: \qquad x_i = \sum_{j=1}^{i} \mu_{ij} x'_j \qquad (\mu_{11} = \lambda;\ i = 1, 2, \cdots, n-1)$$

therefore be assumed to be given in the form

$$C_{n-1}: \quad \begin{aligned} x_1 &= \lambda x'_1, \\ x_i &= \varepsilon_i x'_{i-1} + \lambda x'_i \quad (\varepsilon_i = 0 \text{ or } 1;\ i = 2, 3, \cdots, n-1). \end{aligned}$$

Whenever an ε is zero, C_{n-1} is thereby broken into an open product. If k ε's are zero, C_{n-1} has $k+1$ component substitutions in which no ε is zero. The variables of C_{n-1} may be permuted in such a way that, as we look down the principal diagonal, each of the $k+1$ components is on as many or more variables as the component before it. This arrangement removes any difficulty that may arise in making the determinant of the next transformation different from zero. Now M has the form

$$\begin{aligned} x_1 &= \lambda x'_1, \\ x_i &= \varepsilon_i x'_{i-1} + \lambda x'_i \qquad (\varepsilon_i = 0 \text{ or } 1;\ i = 2, 3, \cdots, s-1), \end{aligned}$$

$$
\begin{aligned}
M:\quad x_s &= \lambda x'_s\,,\\
x_i &= x'_{i-1} + \lambda x'_i \qquad (\varepsilon_i = 1\,;\ i = s+1\,,\ s+2\,,\ \cdots, n-1)\,,\\
x_n &= \sum_{j=1}^{n-1} \mu_j x'_j + \lambda x'_n\,.
\end{aligned}
$$

Assume that

$$(1) \qquad \mu_{n-1} \neq 0\,.$$

In order to transform the last $n-s+1$ equations of M into

$$
\begin{aligned}
y_n &= y'_{n-1} + \lambda y'_n\,,\\
y_{n-1} &= y'_{n-2} + \lambda y'_{n-1}\,,\\
&\cdots\cdots\cdots\cdots\\
y_{s+1} &= y'_s + \lambda y'_{s+1}\,,\\
y_s &= \lambda y'_s\,,
\end{aligned}
$$

it is only necessary to put

$$
\begin{aligned}
y_n &= x_n\,,\\
y_{n-1} &= \sum_{j=1}^{n-1} \mu_j x_j\,,\\
y_{n-i} &= \sum_{j=1}^{n-1} \mu_j \varepsilon_j \varepsilon_{j-1} \cdots \varepsilon_{j-i+2} x_{j-i+1} \qquad (i = 2\,,\ 3\,,\ \cdots\ n-s)\,.
\end{aligned}
$$

If the other variables of M are unchanged we have a substitution of non-zero determinant by which M is transformed into C.

It may be that

$$(2) \qquad \mu_{n-1} = 0\,.$$

In this case it is easy to transform M into an open product, each of whose components can, according to our assumption, be transformed into the desired form. Put

$$y_n = x_n - \sum_{i=s}^{n-1} \mu_{i-1} x_i\,,$$

and leave the other variables of M unchanged. Then

$$y_n = \sum_{i=1}^{s-1} \mu_i x'_i + \lambda y'_n$$

takes the place of the n^{th} equation of M. In the new substitution the variables x_s, x_{s+1}, $\cdots$, x_{n-1} are replaced by linear functions of x'_s, x'_{s+1},

$\cdots, x'_{n-1}$ only, so that M has been transformed, as proposed, into an open product.

It is now evident that any substitution can be transformed into a *canonical form,* that is, into an open product of substitutions such as

$$\begin{aligned} x_1 &= \lambda x'_1 , \\ x_2 &= x'_1 + \lambda x'_2 , \\ x_3 &= x'_2 + \lambda x'_3 , \\ &\cdots\cdots \\ x_t &= x'_{t-1} + \lambda x'_t . \end{aligned} \tag{3}$$

In § 2 we defined the product of two substitutions and saw that it is a substitution whose determinant is the product of the determinants of the two given factors. A substitution has an inverse if its determinant is not zero. Then positive and negative powers of substitutions of non-zero determinant may be defined as was done in § 1 for the special case of permutations. A substitution A is of finite order g if A^g is the identity,

$$x_i = x'_i \qquad (i = 1, 2, \cdots, n),$$

and if g is the smallest positive whole number for which this is true.

The r^{th} power of (3) is

$$\begin{aligned} x_1 &= \lambda^r x'_1 , \\ x_2 &= r\lambda^{r-1} x'_1 + \lambda^r x'_2 , \\ &\cdots\cdots\cdots\cdots ; \end{aligned}$$

hence:

II. A canonical substitution is of finite order g only if it is a multiplication in which the multipliers are g$^{\text{th}}$ *roots of unity.*

§ 23.

Substitutions Commutative with a Canonical Substitution.

Let L be a substitution in canonical form with equal multipliers grouped together along the principal diagonal, first r equal multipliers λ_1, then $s - r$ equal multipliers λ_{r+1}, and so on:

$$L: \qquad x_i = \varepsilon_i x'_{i-1} + \lambda_i x'_i \qquad \begin{aligned} &(\varepsilon_i = 0 \text{ or } 1 ;\ i = 1, 2, \cdots, n ; \\ &\varepsilon_{k+1} = 0 ;\ k = 0, r, s, \cdots, n) . \end{aligned}$$

Let

$$A: \qquad x_i = \sum_{j=1}^{n} a_{ij} x'_j \qquad (i = 1, 2, \cdots, n)$$

be any substitution on n variables commutative with L. The condition that

$$LA = AL$$

is

$$\varepsilon_i a_{i-1,j} + \lambda_i a_{ij} = a_{i,j+1}\varepsilon_{j+1} + a_{ij}\lambda_j \qquad (i, j = 1, 2, \cdots, n),$$

or better,

$$(1) \qquad (\lambda_i - \lambda_j) a_{ij} = a_{i,j+1}\varepsilon_{j+1} - \varepsilon_i a_{i-1,j}.$$

This equation says that a_{ij} is zero when λ_i and λ_j are unequal, provided the coefficients just above and just to the right of a_{ij} are both zero. Then it follows that every a_{ij} above the principal diagonal, for which $\lambda_i \neq \lambda_j$, is zero.

Moreover, every a_{ij} below the principal diagonal, for which $\lambda_i \neq \lambda_j$, is zero if

$$(2) \qquad a_{k+1,j} = 0 \qquad (j = 1, 2, \cdots, k;\ k = r, s, \cdots, n),$$

and

$$(3) \qquad a_{ik} = 0 \qquad (i = k+1, k+2, \cdots, n;\ k = r, s, \cdots, n).$$

We have to prove that (2) and (3) are true. Since

$$\varepsilon_{r+1} = \varepsilon_{s+1} = \cdots = \varepsilon_{n+1} = 0,$$

$$(4) \quad a_{k+1,j}(\lambda_{k+1} - \lambda_j) = a_{k+1,j+1}\varepsilon_{j+1} \quad (j = 1, 2, \cdots, k;\ k = r, s, \cdots, n),$$

$$(5) \quad a_{ik}(\lambda_i - \lambda_k) = -\varepsilon_i a_{i-1,k} \qquad (i = k+1, k+2, \cdots, n;\ k = r, s, \cdots, n),$$

from which (2) and (3) follow. Hence:

I. If

$$A: \qquad x_i = \sum_{j=1}^{n} a_{ij} x'_j \qquad (i = 1, 2, \cdots, n)$$

is commutative with

$$x_i = \varepsilon_i x'_{i-1} + \lambda_i x'_i \quad (\varepsilon_1 = 0;\ \varepsilon_i = 0 \text{ or } 1;\ i = 1, 2, \cdots, n),$$

then

$$a_{ij} = 0$$

whenever

$$\lambda_i \neq \lambda_j.$$

We have no occasion to determine A completely, but add a theorem of which use will be made:

II. If a canonical substitution L replaces $x_1, x_{b+1}, \cdots, x_{m+1}$ by $\lambda x'_1, \lambda x'_{b+1}, \cdots, \lambda x'_{m+1}$, and every other variable x_i by $x'_{i-1} + \lambda x'_i$, any substitution commutative with L transforms $x_1, x_{b+1}, \cdots, x_{m+1}$, into linear functions of $x'_1, x'_{b+1}, \cdots, x'_{m+1}$.

When A is commutative with a canonical substitution L of variety one, (1) reduces to

$$a_{i,\,j+1}\varepsilon_{j+1} = \varepsilon_i a_{i-1,\,j}\,. \tag{6}$$

By hypothesis

$$\varepsilon_{k+1} = 0 \qquad (k = 0\,,\ b\,,\ c\,,\ \cdots,\ n)\,,$$

and every other ε is unity. At least one ε is unity unless L is a similarity substitution. If we put $k+1$ for i in (6), it becomes

$$a_{k+1,\,j+1}\varepsilon_{j+1} = 0 \qquad (k = 0\,,\ b\,,\ c\,,\ \cdots,\ m\,,\ n)\,.$$

Therefore

$$a_{k+1,\,j+1} = 0 \qquad (j \neq 0\,,\ b\,,\ \cdots,\ m;\ k = 0\,,\ b\,,\ \cdots,\ m)\,.$$

§ 24.

Group of Substitutions.

The g distinct linear homogeneous substitutions $A\,, B\,, C\,, \cdots$ on n variables constitute a *group of substitutions* if, and only if, they can be so arranged in a one-to-one correspondence to the permutations $A', B', C', \cdots$ of some group (§ 4) of order g, that ST corresponds to $S'T'$ $(S\,, T = A\,, B\,, C\,, \cdots)$.

That groups of substitutions exist which are not merely groups of permutations (§ 2) is evident from this example:

The four substitutions

$$x = x'\,,\quad x = ix'\,,\quad x = -x'\,,\quad x = -ix'\,, \qquad (i = \sqrt{-1})$$

are arranged in one-to-one correspondence to

$$1,\quad (abcd)\,,\quad (ac)(bd)\,,\quad (adcb)\,,$$

and therefore constitute a group.

We shall use the term *linear group* as a synonym for "group of linear substitutions" or "group of substitutions," and where no undesirable ambiguity is introduced, the word *group* will be used for both linear groups and groups of permutations, that is, for all linear groups.

The definitions of "order of a group," "Abelian group," "cyclic group," "diedral group," "generators," "subgroup," "Sylow subgroup," "conjugates," "complete set of conjugates," "cross-cut," "central," "permutable groups," "direct product of two groups," "isomorphism," "homomorphism," "equivalent groups," "similar groups," "complete groups," may now be extended to groups of substitutions, if in each definition we replace "permutation" by "substitution."

Every group is isomorphic to a regular group, and in consequence the greater part of the theorems proved in Chapters I and II hold true for linear groups.

The number of variables transformed by a substitution is its *degree.* The number of variables transformed by the substitutions of a group may be called the *degree of the group.*

A group of degree n is *reducible* when s $(< n)$ linear functions of the variables exist which are transformed into linear functions of themselves by every substitution of the group. If this condition is not satisfied the group is *irreducible.*

Every group of permutations is reducible because the sum of its n variables is invariant under it.

I. Only similarity substitutions are commutative with every substitution of an irreducible group.

Let S be a substitution commutative with every substitution of a group G. There exists a substitution T of non-zero determinant that transforms S into the canonical form of § 22. By § 23, I and II, either $T^{-1}GT$ is reducible or $T^{-1}ST$ is a similarity substitution. But if G is irreducible, $T^{-1}GT$ is likewise irreducible.

§ 25.

The Sum of Substitutions.

It is possible to give a definition of the *sum* of two substitutions

$$A: \qquad x_i = \sum_{j=1}^{n} a_{ij}x'_j \qquad (i = 1, 2, \cdots, n),$$

and

$$B: \qquad x_i = \sum_{j=1}^{n} b_{ij}x'_j \qquad (i = 1, 2, \cdots, n).$$

The sum $A+B$ is the substitution

$$A+B: \qquad x_i = \sum_{j=1}^{n} (a_{ij}+b_{ij})x'_j \quad (i=1, 2, \cdots, n).$$

The addition of substitutions is commutative:

$$A+B=B+A.$$

If C is a third substitution

$$C: \qquad x_i = \sum_{j=1}^{n} c_{ij}x'_j \qquad (i=1, 2, \cdots, n),$$

the product

$$(A+B)C=AC+BC;$$

for $(A+B)C$ is

$$\begin{aligned} x_i &= \sum_{j=1}^{n}\sum_{k=1}^{n}(a_{ij}+b_{ij})c_{jk}x'_k \\ &= \sum_{j=1}^{n}\sum_{k=1}^{n} a_{ij}c_{jk}x'_k + \sum_{j=1}^{n}\sum_{k=1}^{n} b_{ij}c_{jk}x'_k \qquad (i=1, 2, \cdots, n). \end{aligned}$$

Similarly

$$C(A+B)=CA+CB.$$

I. In the sum of the substitutions of an irreducible group every coefficient is zero.

The sum of all the substitutions of an irreducible group is commutative with every substitution of the group and is, by § 24, I, a similarity substitution. Since multiplication of this sum by a substitution of the group merely permutes its terms, every coefficient of the sum is zero.

In particular, if $\chi_1, \chi_2, \cdots, \chi_g$ are the characteristics of the substitutions of an irreducible group of order g,

$$\sum_{i=1}^{g} \chi_i = 0. \tag{1}$$

II. The sum of the substitutions of a complete set of conjugates in an irreducible group is a similarity substitution.

In any group the sum of all the substitutions of a complete set of conjugates is a substitution commutative with every substitution of the group. In an irreducible group the sum of the g_i substitutions that constitute a complete set of conjugates is therefore a similarity substitution whose characteristic is $g_i\chi_i$.

If

$$C_i = S_1 + S_2 + \cdots + S_{g_i}$$

is the sum of one complete set of conjugates and

$$C_j = T_1 + T_2 + \cdots + T_{g_j}$$

is another in the same group G of degree n, the product

$$C_i C_j = \sum_{s=1}^{g_i} \sum_{t=1}^{g_j} S_s T_t .$$

Since the substitutions $S_s T_t$ are merely permuted among themselves on transformation by substitutions of G, all conjugates of any substitution $S_s T_t$ occur in the sum $C_i C_j$. If one member of the complete set of conjugates to which $S_s T_t$ belongs occurs c_{ijk} times in the sum $C_i C_j$, each member of the set occurs as often. Hence

$$C_i C_j = \sum_{k=1}^{h} c_{ijk} C_k ,$$

if C_k is the sum of the substitutions of the k^{th} conjugate set and if there are h complete sets of conjugate substitutions in G. Then, if we equate multipliers from the two sides of this identity,

$$\frac{g_i \chi_i}{n} \; \frac{g_j \chi_j}{n} = \sum_{k=1}^{h} c_{ijk} \frac{g_k \chi_k}{n} . \tag{2}$$

§ 26.

The Hermitian Form.

The s linear functions of the variables that a reducible group transforms into linear functions of themselves may, if they are linearly independent, be taken for new variables, $y_1, y_2, \cdots, y_s$, say. Then the first s equations of every substitution of the given group are on these s variables only.

What is meant by linear independence of s functions $f_1, f_2, \cdots, f_s$ is this: if s numbers $a_1, a_2, \cdots, a_s$ do not exist that satisfy the condition

$$a_1 f_1 + a_2 f_2 + \cdots + a_s f_s = 0 ,$$

$f_1, f_2, \cdots, f_s$ are said to be *linearly independent.* If $f_1, f_2, \cdots, f_s$ are linear functions of n $(> s)$ variables $x_1, x_2, \cdots, x_n$, all the determinants of order s of the matrix of the coefficients of $f_1, f_2, \cdots, f_s$ vanish in case

$$a_1 f_1 + a_2 f_2 + \cdots + a_s f_s = 0 .$$

But if $f_1, f_2, \cdots, f_s$ are linearly independent, not all the determinants of the matrix vanish, so that a substitution of non-zero determinant can be set up that will transform every substitution of the group into the indicated form. If the s given functions are not linearly independent, s' $(1 \leqq s' < s)$ of them are linearly independent and we may as well assume that the s functions are linearly independent in the first place.

The reducible group may be further transformed so that every substitution in it appears as an open product of two components, one on the variables $y_1, y_2, \cdots, y_s$, and the other on $y_{s+1}, y_{s+2}, \cdots, y_n$. To bring this about we shall introduce the Hermitian invariant.

A bilinear form

$$\sum_{i=1}^{n} \sum_{j=1}^{n} c_{ij} x_i \bar{x}_j \qquad (c_{ji} = \bar{c}_{ij})$$

is an *Hermitian form.* By $\bar{z}$ is meant the conjugate imaginary of the complex number z. If the Hermitian form is zero only for

$$x_1 = x_2 = \cdots = x_n = 0 ,$$

we shall call it a *non-zero* form.

A non-zero form can be transformed into

$$x_1 \bar{x}_1 + x_2 \bar{x}_2 + \cdots + x_n \bar{x}_n ,$$

by the following process:

Let the given form be

$$I_n = c_{nn} x_n \bar{x}_n + x_n \sum_{j=1}^{n-1} c_{nj} \bar{x}_j + \bar{x}_n \sum_{i=1}^{n-1} c_{in} x_i + \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} c_{ij} x_i \bar{x}_j$$

$$(c_{ji} = \bar{c}_{ij}) .$$

Since $I_n = c_{nn}$ when

$$x_n - 1 = x_{n-1} = \cdots = x_2 = x_1 = 0 ,$$

c_{nn} is not zero. Hence I_n may be written

$$I_n = \sum_{i=1}^{n} c_{in} x_i \sum_{j=1}^{n} c_{nj} \bar{x}_j / c_{nn} + I_{n-1} ,$$

where

$$I_{n-1} = \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} (c_{ij} - c_{in} c_{nj} / c_{nn}) x_i \bar{x}_j$$

$$= \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} d_{ij}x_i\bar{x}_j .$$

Now I_{n-1} is a non-zero Hermitian form in $n-1$ variables, for $d_{ji} = \bar{d}_{ij}$, and any simultaneous values of $x_1, x_2, \cdots, x_{n-1}$, not all zero, which make I_{n-1} zero, will, with x_n determined by

$$x_n = -\sum_{i=1}^{n-1} c_{in}x_i/c_{nn} ,$$

make I_n also zero, contrary to hypothesis. If, therefore, we put

$$y_n = \sum_{i=1}^{n} c_{in}x_i/\sqrt{c_{nn}} ,$$

then

$$I_n = y_n\bar{y}_n + I_{n-1} ,$$

and I_{n-1} may be treated in the same way; and so on. Hence:

I. A non-zero Hermitian form in n variables can be transformed, by means of a normal substitution of non-zero determinant, into

$$y_1\bar{y}_1 + y_2\bar{y}_2 + \cdots + y_n\bar{y}_n .$$

§ 27.

The Composition of Two Homomorphic Groups.

Let G and G' be two groups on distinct sets of variables $x_1, x_2, \cdots, x_n$ and $y_1, y_2, \cdots, y_m$, between which there exists a given homomorphism. Let

$$A: \qquad x_i = \sum_{j=1}^{n} a_{ij}x'_j \qquad (i = 1, 2, \cdots, n)$$

and

$$A': \qquad y_h = \sum_{k=1}^{m} a'_{hk}y'_k . \qquad (h = 1, 2, \cdots, m)$$

be two corresponding substitutions. If the n equations of A are multiplied by the m equations of A', we get

$$A'': \; x_iy_h = \sum_{j=1}^{n} \sum_{k=1}^{m} a_{ij}a'_{hk}x'_jy'_k \quad (i = 1, 2, \cdots, n;\; h = 1, 2, \cdots, m) .$$

This is a linear substitution on the nm products x_iy_h, the result of *compounding* A and A'. Let a substitution B'' be formed in the same way from the two corresponding substitutions B and B':

$$B'': \quad x_jy_k = \sum_{s=1}^{n} \sum_{t=1}^{m} b_{js}b'_{kt}x'_sy'_t .$$

The product $A''B''$ is

$$x_i y_h = \sum_{j=1}^{n} \sum_{k=1}^{m} \sum_{s=1}^{n} \sum_{t=1}^{m} a_{ij} a'_{hk} b_{js} b'_{kt} x'_s y'_t$$
$$= \sum_{j=1}^{n} \sum_{s=1}^{n} a_{ij} b_{js} x'_s \quad \sum_{k=1}^{m} \sum_{t=1}^{m} a'_{hk} b'_{kt} y'_t \,,$$

so that the substitutions A'', B'', $\cdots$, f in number, say, are each the identity or constitute a group of order $\leqq f$, homomorphic to G and to G', on the nm variables $x_i y_h$, arising from the *composition* of the two groups G and G'. If G (of order g) is isomorphic to G', or $(h, 1)$ isomorphic to G', $f = g$. Let us introduce a symbol for this composition:

$$G \times G' .$$

This need not be confused with GG' (§ 8) or with $\{G, G'\}$ (§ 4). It should be borne in mind that $G \times G'$ is not in general unique, but depends on the correspondence between G and G'.

It may be that $G \times G'$, on the nm variables $X_i Y_h$ has an invariant

$$\sum_{i=1}^{n} \sum_{j=1}^{m} c_{ij} X_i Y_j .$$

If so, it can be put in the form

$$(1) \qquad x_1 y_1 + x_2 y_2 + \cdots + x_s y_s ,$$

where $x_1, x_2, \cdots, x_s$ and $y_1, y_2, \cdots, y_s$ are linearly independent functions of the first degree of the variables $X_1, X_2, \cdots, X_n$, and $Y_1, Y_2, \cdots, Y_m$, respectively. Then we may introduce the new variables $x_1, x_2, \cdots, x_n$ and $y_1, y_2, \cdots, y_m$ in G and G'. Let A and A', as in the preceding paragraph, be corresponding substitutions of G and G', and A'' the substitution resulting from their composition. Now A'' transforms (1) into

$$\sum_{i=1}^{s} \sum_{j=1}^{n} \sum_{k=1}^{m} a_{ij} a'_{ik} x'_j y'_k = \sum_{h=1}^{s} x'_h y'_h ;$$

whence, for $j = 1, 2, \cdots, n$, and $k = 1, 2, \cdots, m$,

$$(2) \qquad \sum_{i=1}^{s} a_{ij} a'_{ik} = 1 \qquad (j = k \leqq s) ,$$

$$(3) \qquad \sum_{i=1}^{s} a_{ij} a'_{ik} = 0 \qquad (j \neq k ;\ \text{or}\ j = k > s) .$$

For a given subscript k $(> s)$ we have the n equations

$$\sum_{i=1}^{s} a_{ij} a'_{ik} = 0 \qquad (j = 1, 2, \cdots, n) .$$

Not all the determinants of order s of the matrix

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ a_{s1} & a_{s2} & \cdots & a_{sn} \end{vmatrix}$$

vanish, because the determinant of A is not zero. Hence

$$a'_{ik} = 0 \qquad (i = 1, 2, \cdots, s; \; k = s+1, s+2, \cdots, n).$$

Similarly,

$$a_{ij} = 0 \qquad (i = 1, 2, \cdots, s; \; j = s+1, s+2, \cdots, n).$$

This means that in every substitution of G and G', the first s variables are transformed into linear functions of themselves.

For $s < n$ the following theorem has been proved true:

I. If a group G on the variables $x_1, x_2, \cdots, x_n$ is compounded with a group G' on the variables $y_1, y_2, \cdots, y_m$, and if

$$(4) \qquad \sum_{i=1}^{s} \sum_{j=1}^{n} e_{ij} x_j \sum_{k=1}^{m} f_{ik} y_k \qquad (s < n)$$

is invariant under $G \times G'$, G is reducible.

If G is irreducible, $s = n$; in addition, let $m = n$, as it is if G' is also irreducible. Now $G \times G'$ has, we say, one invariant

$$(5) \qquad x_1 y_1 + x_2 y_2 + \cdots + x_n y_n,$$

and may possibly have another:

$$(6) \qquad \sum_{i=1}^{n} \sum_{j=1}^{n} d_{ij} x_i y_j .$$

If it has,

$$(7) \qquad \sum_{i=1}^{n} \sum_{j=1}^{n} d_{ij} x_i y_j - \lambda \sum_{k=1}^{n} x_k y_k,$$

where λ is an arbitrary constant, is also an invariant of $G \times G'$. But if λ is a root of the equation

$$(8) \qquad \begin{vmatrix} d_{11} - t, & d_{21}, & \cdots & d_{n1}, \\ d_{12}, & d_{22} - t, & \cdots & d_{n2}, \\ \cdot & \cdot & \cdots & \cdot \\ d_{1n}, & d_{2n}, & & d_{nn} - t, \end{vmatrix} = 0,$$

the n functions

$$\sum_{i=1}^{n} d_{ij}x_j - \lambda x_j \qquad (j = 1, 2, \cdots, n)$$

are not linearly independent, so that (7) can be put in the form (4), and therefore G should be reducible. Hence:

II. If G and G' (as given in I) are both irreducible groups, $G \times G'$ has not two linearly independent invariants of the first degree.

§ 28.

The Hermitian Invariant.

Let the variables and coefficients of every substitution of G (of order g) be replaced by their conjugate imaginaries; the resulting substitutions constitute a group $\bar{G}$ on the n variables $\bar{x}_1, \bar{x}_2, \cdots, \bar{x}_n$, isomorphic to G. When this change is made in a substitution A, the new substitution $(\bar{A})$ is called the *conjugate imaginary substitution to A*. Then $G \times \bar{G}$, formed by compounding each substitution of G with its conjugate imaginary substitution, is on the n^2 variables $x_i\bar{x}_j$.

Now transform $x_i\bar{x}_i$ by all the substitutions of $G \times \bar{G}$ and add. This summation is indicated by $\sum_a$. We have, restoring the unaccented variables,

$$I = \sum_a \sum_{j=1}^{n} \sum_{k=1}^{n} a_{ij}\bar{a}_{ik}x_j\bar{x}_k \tag{1}$$

$$= \sum_a \sum_{j=1}^{n} a_{ij}x_j \sum_{k=1}^{n} \bar{a}_{ik}\bar{x}_k \tag{2}$$

$$= \sum_{j=1}^{n} \sum_{k=1}^{n} x_j\bar{x}_k \sum_a a_{ij}\bar{a}_{ik}\,. \tag{3}$$

This function is invariant under $G \times \bar{G}$ and does not vanish identically, for (2) shows it to be a sum of real positive numbers. In fact, it is not zero unless each of the s $(\leqq n)$ variables $x_1, x_2, \cdots$ actually present in it is zero. Hence,

I. If the substitutions of a group are compounded with their conjugate imaginaries, the resulting substitutions transform at least one non-zero Hermitian form into itself.

The Hermitian form

$$\sum_a \sum_{j=1}^{n} a_{ij}x_j \sum_{k=1}^{n} \bar{a}_{ik}\bar{x}_k$$

certainly contains the variable x_i, and therefore

$$J = \sum_{a} \sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{k=1}^{n} a_{ij}\bar{a}_{ik}x_j\bar{x}_k$$

contains the n variables $x_1, x_2, \cdots, x_n$, and is a non-zero Hermitian form invariant under $G \times \bar{G}$, or, as we may say for the sake of brevity, an *Hermitian invariant of G*. Let G be transformed by the substitution which transforms J into

$$(4) \qquad I = x_1\bar{x}_1 + x_2\bar{x}_2 + \cdots + x_n\bar{x}_n .$$

If

$$A: \qquad x_i = \sum_{j=1}^{n} a_{ij}x'_j \qquad (i = 1, 2, \cdots, n)$$

is a substitution of the transformed group, equations (2) and (3) of § 27 become, for $s = n$,

$$(5) \qquad \sum_{i=1}^{n} a_{ij}\bar{a}_{ik} = 1 \qquad (j = k),$$

$$(6) \qquad \sum_{i=1}^{n} a_{ij}\bar{a}_{ik} = 0 \qquad (j \neq k).$$

A substitution whose coefficients satisfy equations (5) and (6) is said to be in *unitary* form. From these equations

$$(7) \qquad \bar{a}_{ik} = \frac{A_{ik}}{|A|},$$

where A_{ik} is the minor of a_{ik} in the determinant $|A|$ of the substitution A. Hence the inverse of A is

$$A^{-1}: \qquad x_k = \sum_{i=1}^{n} \bar{a}_{ik}x'_i \qquad (k = 1, 2, \cdots, n).$$

To sum up:

II. Any group of degree n may be transformed into a group for which

$$x_1\bar{x}_1 + x_2\bar{x}_2 + \cdots + x_n\bar{x}_n$$

is an Hermitian invariant, and in which therefore every substitution assumes the unitary form.

Going back to § 27, let it be assumed that G, of degree n, and G' are irreducible groups, that G is in unitary form and that the variables of G' are so chosen that

$$x_1y_1 + x_2y_2 + \cdots + x_ny_n$$

is invariant under $G \times G'$. Then G' is also of degree n. The solutions of the n equations (for a given k)

$$\sum_{i=1}^{n} a_{ik} a'_{ik} = 1 ,$$

$$\sum_{i=1}^{n} a_{ij} a'_{ik} = 0 \qquad (j = 1, 2, \cdots, k-1, k+1, \cdots, n) ,$$

are

$$a'_{ik} = \bar{a}_{ik} \qquad (i = 1, 2, \cdots, n) .$$

Hence,

III. If and only if the irreducible groups G and G′ can be so transformed that corresponding substitutions become conjugate imaginaries, G × G′ has an invariant of the first degree.

§ 29.

The Complete Reduction of a Reducible Group.

We return to the reducible group of § 26, which transforms the s variables $x_1, x_2, \cdots, x_s$ into linear functions of themselves. This property is retained if the group is subjected to transformation by a substitution in normal form. Then let it be so transformed that

$$x_1\bar{x}_1 + x_2\bar{x}_2 + \cdots + x_n\bar{x}_n$$

becomes an Hermitian invariant for it. All its substitutions are unitary, and the determinant of each has the form

$$\begin{vmatrix} S & O \\ R & T \end{vmatrix} ,$$

where the elements of S and T are squares of s^2 and $(n-s)^2$ elements, respectively, R is a rectangle of s columns and $n-s$ rows, while all the other elements are zero.

The minor (a determinant of the $n - 1$st order) of any element in R is zero, so that by equation (7) of § 28,

$$\bar{a}_{ik} = 0 \qquad (i = s+1, s+2, \cdots, n; \; k = 1, 2, \cdots, s) .$$

Hence every element of R is zero and every substitution of the reducible group is the open product of two components on s and $n-s$ variables, respectively. The group breaks into two constituents (one of which may be the identity) with no variable in common. One constituent at least is a group, and may itself be reducible; if so, it in turn may be broken into two constituents just as was done to the original group; and so on. Finally our reducible group will appear with a number of constituents, no two of which have a variable in common, and each either an irreducible group or the identity. In this event the group is said to be *completely reduced.*

The sum of the characteristics of each constituent irreducible group is zero (§ 25, I.), while a constituent on one variable that is merely the identity has the characteristic unity. Therefore, if exactly k constituents, when a group of order g is completely reduced, are not groups, but the identity repeated g times,

$$\sum_{i=1}^{g} \chi_i = kg. \tag{1}$$

In the case of a transitive permutation group, $k=1$ (§ 19).

Then if χ_i and χ'_i are the characteristics of the corresponding substitutions of two homomorphic irreducible groups G and G' (§ 28, III),

$$\sum_{i=1}^{f} \chi_i \chi'_i = 0 \tag{2}$$

(where f is the number of substitutions, not necessarily distinct, in $G \times G'$), unless

$$\chi'_i = \bar{\chi}_i ,$$

in which case $f=g$, the order of G, and

$$\sum_{i=1}^{g} \chi_i \bar{\chi}_i = g. \tag{3}$$

As an example, the symmetric group of degree 3 may be completely reduced. Since any group on one variable is Abelian, this symmetric group will break into an irreducible constituent on two variables and the identity on one variable. Transform $\{(x_1 x_2),\ (x_1 x_3)\}$ by the substitution

$$y_1 = x_1 + x_2 + x_3 ,$$
$$y_2 = x_1 + \alpha x_2 + \alpha^2 x_3 ,$$
$$y_3 = x_1 + \alpha^2 x_2 + \alpha x_3 ,$$

where α is a primitive cube root of unity. The transforms of $(x_1 x_2)$ and $(x_1 x_3)$ are, respectively,

$$y_1 = y'_1 , \quad y_2 = \alpha y'_3 , \quad y_3 = \alpha^2 y'_2 ,$$

and

$$y_1 = y_1' , \quad y_2 = \alpha^2 y_3' , \quad y_3 = \alpha y_2' .$$

The six substitutions of this reduced group are *monomial,* a term that explains itself. The second and third constituents of the subgroup of order 3 are equivalent, but dissimilar.

§ 30.

Reduction of the Regular Group.

It is now possible to extend Theorem III of § 28 if for G a reducible group is in question. It can be assumed that G is completely reduced. Then $G \times G'$ has just as many linearly independent invariants of the first degree as G has irreducible constituents whose substitutions, after appropriate transformation, are conjugate imaginaries of the corresponding substitutions of the irreducible unitary group G'. Let there be l of these groups each equal to $\bar{G}'$. We shall speak of them as a *cluster* of l similar irreducible groups in the completely reduced group G. If now $\chi_1, \chi_2, \cdots, \chi_g$ are the characteristics of the substitutions of G and if the characteristics of G' which correspond to those of G in setting up $G \times G'$ are $\chi_1', \chi_2', \cdots, \chi_g'$,

$$(1) \qquad \sum_{i=1}^{g} \chi_i \chi_i' = lg .$$

A remarkable property of the regular group (§ 12) follows immediately. All the characteristics of a regular group are zero except that of the identity, which is g, the order of the group. Then if G' is any irreducible group of degree n_j (in unitary form if we like), isomorphic to the regular group G or to a quotient group of G; in other words, if G' is an irreducible *representation* of G on n_j variables, we have

$$\sum_{i=1}^{g} \chi_i \chi_i' = n_j g .$$

The identity on one variable is called the *identical representation.* Hence,

I. The complete reduction of a regular group can be so effected that any irreducible constituent of degree n_j is repeated n_j times in such a way that each of its substitutions has just n_j components of degree n_j identically the same. Furthermore, every irreducible representation of the group is found among the constituents.

An irreducible constituent, not one of this cluster of n_j similar constituents, is dissimilar to any one of them, the implied correspondence being the actual isomorphism between irreducible constituents of the reduced regular group. In addition to the identical representation let there be exactly $k-1$ dissimilar irreducible representations of G. Then

$$\sum_{j=1}^{k} n_j^2 = g .$$

Let $\chi_1^j, \chi_2^j, \cdots$ be the characteristics of the substitutions of an irreducible constituent of the j^{th} cluster in the order in which the substitutions of the constituent correspond to substitutions of G. Let χ_1 (as usual) be the characteristic of the identity, so that $\chi_1^j = n_j$, $\chi_1^1 = n_1 = 1$.

If we mean thereby that no linear equation with constant coefficients:

$$\sum_{j=1}^{k} A_j \chi_i^j = 0 ,$$

holds for every value of i, we can say:

II. The k sets of group characteristics $\chi_i^1, \chi_i^2, \cdots, \chi_i^k$ $(i=1, 2, \cdots, g)$ of a given group of order g are linearly independent.

For if

$$\sum_{j=1}^{k} A_j \chi_i^j = 0 \qquad (i=1, 2, \cdots, g) ,$$

$$\sum_{i=1}^{g} \bar{\chi}_i^w \sum_{j=1}^{k} A_j \chi_i^j = 0 ,$$

$$\sum_{j=1}^{k} A_j \sum_{i=1}^{g} \bar{\chi}_i^w \chi_i^j = 0 ,$$

and by § 29, (2) and (3), this is

$$A_w g = 0 \qquad (w=1, 2, \cdots, k) .$$

III. Two isomorphic irreducible groups are similar if and only if the characteristics of corresponding substitutions are equal.

For by Theorem II, two irreducible groups that are isomorphic and dissimilar, being representations of the same group, cannot have the same characteristics unless they occur in different sequence for the two groups.

IV. In the completely reduced form of a regular group there are just as many dissimilar irreducible constituents as the regular group has complete sets of conjugate permutations.

Transformation by a substitution T completely reduces the regular group G, let us say. Multiply each of the g_i substitutions of the i^{th} conjugate set of $T^{-1}GT$ by a similarity substitution whose multiplier is an arbitrary constant v_i $(i=1, 2, \cdots, h)$, and call the sum of all the g

$$\sum_{j=1}^{k} n_j$$

substitutions so affected, S. The substitution S is the open product of components, each on the variables of an irreducible constituent of $T^{-1}GT$, and each of the components of S is therefore (§ 24, I) a similarity substitution with the multiplier

$$\alpha_j = \sum_{i=1}^{h} v_i g_i \chi_i^j / \chi_1^j \qquad (j = 1, 2, \cdots, k).$$

These k multipliers are linearly independent. For if

$$\sum_{j=1}^{k} A_j \alpha_j = 0,$$

$$\sum_{j=1}^{k} (A_j / \chi_1^j) \chi_i^j = 0 \quad (i = 1, 2, \cdots, h),$$

contradicting Theorem II.

Since at most h linear homogeneous functions of h variables are linearly independent, $k \leqq h$.

In the sum of all the coefficients of the regular group every coefficient is unity. Therefore TST^{-1} has just h arbitrary coefficients $v_1, v_2, \cdots, v_h$, and these coefficients are linear functions of $\alpha_1, \alpha_2, \cdots, \alpha_k$. Then $h \leqq k$, so that finally

$$k = h.$$

Another way of stating Theorem II is this:

V. The determinant

$$|\chi_i^j| \qquad (i, j = 1, 2, \cdots, h)$$

does not vanish.

The following relations between the characteristics follow from our discussion of the regular group:

$$\sum_{j=1}^{h} (\chi_1^j)^2 = g, \tag{2}$$

and

$$\sum_{j=1}^{h} \chi_i^j \chi_1^j = 0, \tag{3}$$

when $i \neq 1$.

It is interesting to notice what happens to the regular Abelian group when it is completely reduced. By Theorem IV, each irreducible constituent is on one variable, that is:

VI. An Abelian group can be so transformed that every substitution assumes the canonical form.

§ 31.

Other Relations Between the Characteristics.

We recall from § 25 the identity

$$g_i\chi_i^w g_j\chi_j^w = \chi_1^w \sum_{k=1}^{h} c_{ijk} g_k \chi_k^w \,, \tag{1}$$

and the meaning of the coefficients c_{ijk}. For example, c_{ij1} is the number of times the conjugate set consisting of the identity alone recurs when all the substitutions of the i^{th} conjugate set are multiplied into those of the j^{th} set. Thus

$$c_{ij1} = 0$$

unless the substitutions of the j^{th} set are the inverses of the substitutions of the i^{th} set. In the latter case

$$c_{ij1} = g_i = g_j \,,$$

and

$$\chi_j^w = \bar{\chi}_i^w \,.$$

Now sum (1) for the h linearly independent sets of characteristics that occur in the complete reduction of the regular group:

$$\begin{aligned} g_i g_j \sum_{w=1}^{h} \chi_i^w \chi_j^w &= \sum_{w=1}^{h} \sum_{k=1}^{h} c_{ijk} g_k \chi_1^w \chi_k^w \\ &= \sum_{k=1}^{h} c_{ijk} g_k \sum_{w=1}^{h} \chi_1^w \chi_k^w \\ &= g c_{ij1} \,, \end{aligned}$$

If we use § 30, (2) and (3). Therefore,

$$g_i \sum_{w=1}^{h} \chi_i^w \bar{\chi}_i^w = g \,, \tag{2}$$

but

$$\sum_{w=1}^{h} \chi_i^w \chi_j^w = 0 \,, \tag{3}$$

when $\chi_j^w \neq \bar{\chi}_i^w$.

With the aid of these equations certain relations between the characteristics of a group and those of any one of its subgroups can be developed.

Let G be a group of order g and let G' of order g' be one of its subgroups. Let χ_i^u $(u = 1, 2, \cdots, h)$ and ψ_i^v $(v = 1, 2, \cdots, h')$ be the sets of characteristics of G and G', respectively. They are the characteristics of the dissimilar irreducible constituents of the regular group isomorphic to G, or to G'. Let Γ_u be that irreducible representation of G whose characteristics are χ_i^u and let Γ_u' be its subgroup that corresponds to G'. Let each irreducible representation of G' occur (without permutation of characteristics) k_{uv} times when Γ_u' is completely reduced. Some of the coefficients k_{uv} may be zero. Then for any substitution of G',

$$\sum_{v=1}^{h'} k_{uv}\psi_i^v = \chi_i^u , \tag{4}$$

or, what is more convenient for our present purpose,

$$\bar{\chi}_i^u = \sum_{v=1}^{h'} k_{uv}\bar{\psi}_i^v .$$

Multiply by ψ_i^w and sum for all the substitutions of G':

$$\begin{aligned} \sum_{i=1}^{g'} \bar{\chi}_i^u\psi_i^w &= \sum_{i=1}^{g'} \psi_i^w \sum_{v=1}^{h'} k_{uv}\bar{\psi}_i^v \\ &= \sum_{v=1}^{h'} k_{uv} \sum_{i=1}^{g'} \bar{\psi}_i^v\psi_i^w \\ &= g'k_{uw} . \qquad (5) \end{aligned}$$

The reduction is by § 30, (1). Now multiply by χ_j^u and sum for all the h sets of characteristics of G:

$$\begin{aligned} \sum_{u=1}^{h} \chi_j^u g' k_{uw} &= \sum_{u=1}^{h} \chi_j^u \sum_{i=1}^{g'} \bar{\chi}_i^u\psi_i^w \\ &= \sum_{i=1}^{g'} \psi_i^w \sum_{u=1}^{h} \bar{\chi}_i^u\chi_j^u . \end{aligned}$$

Hence, by (2) and (3),

$$\sum_{u=1}^{h} k_{uw}\chi_j^u = \frac{g}{g'g_j} \sum \psi_j^w \qquad (w = 1, 2, \cdots, h') , \tag{6}$$

where the second summation extends to the characteristics of those substitutions of G' conjugate under G to a substitution S_j of G whose characteristic is χ_j^u. If S_j has no conjugate in G', the right-hand member of (6) is zero.

CHAPTER IV.

APPLICATIONS OF GROUP CHARACTERISTICS.

§ 32.

Permutation Groups of Degree n and Class n — 1.

The *class* of a group of permutations is the number of letters displaced by those of its permutations which displace the fewest letters.

I. A transitive group of degree n and class n — 1 has an invariant subgroup.

Let g be the order of the transitive group G of degree n and class $n - 1$ in question. Of the n conjugate subgroups that fix one letter of G, no two have a subgroup in common. There are $g - n$ permutations of degree $n - 1$ and $n - 1$ permutations of degree n. Any permutation of degree n permutes all the n subgroups of degree $n - 1$ and order g/n and any permutation of degree $n - 1$ permutes all those subgroups except that one in which it is contained. In consequence, if the subgroup G' of § 31 is one of these subgroups of order g/n, (6) of § 31 becomes

$$(1) \qquad \sum_{u=1}^{h} k_{uw}\chi_i^u = n\psi_1^w\,, \text{ or } \psi_i^w\,,$$

for the identity, or for a permutation of degree $n - 1$, respectively. Putting (§ 31, (4))

$$\chi_i^u = \sum_v k_{uv}\psi_i^v\,,$$

in (1), we have

$$\sum_{u=1}^{h} \sum_v k_{uv}k_{uw}\psi_i^v = \psi_i^w \qquad (i \neq 1)\,,$$

$$\sum_u \sum_v k_{uv}k_{uw}\psi_1^v = n\psi_1^w\,,$$

or

$$(2) \qquad \sum_u \sum_v k_{uv}k_{uw}\psi_i^v = \psi_i^w + \frac{n^2 - n}{g}\psi_1^w \sum_v \psi_i^v\psi_1^v\,,$$

for all the permutations of a subgroup of degree $n - 1$. Comparing the coefficients (§ 30, II) of ψ_i^v,

$$\sum_u (k_{uv})^2 = \frac{n^2 - n}{g}(\psi_1^v)^2 + 1\,,$$

$$\sum_u k_{uv}k_{uw} = \frac{n^2 - n}{g}\psi_1^v\psi_1^w \qquad (w \neq v)\,.$$

Therefore

$$\sum_{u} (k_{uv} - \psi_1^v k_{u1})^2 = (\psi_1^v)^2 + 1 .$$

Now (§ 31, (4))

(3) $$k_{11} = 1 , \quad k_{1v} = 0 \ (v > 1) .$$

Hence

$$(k_{1v} - \psi_1^v k_{11})^2 = (\psi_1^v)^2 \qquad (v > 1) ,$$

and therefore

(4) $$\sum_{u=2}^{h} (k_{uv} - \psi_1^v k_{u1})^2 = 1 \qquad (v > 1) .$$

Hence, for a given $v = b$ (> 1) , there is a certain $u = a$ (> 1) such that

(5) $$k_{ab} - \psi_1^b k_{a1} = \varepsilon \qquad (\varepsilon^2 = 1) ,$$

(6) $$k_{ub} - \psi_1^b k_{u1} = 0 \qquad (u = 2 , 3 , \cdots , a - 1 , a + 1 , \cdots , h) .$$

For any permutation of G of degree n (§31, (6)),

$$\sum_{u=1}^{h} k_{uv} \chi_i^u = 0 \qquad (v = 1 , 2 , \cdots , h') ,$$

Therefore for these $n - 1$ permutations

(7) $$\sum_{u=1}^{h} (k_{ub} - \psi_1^b k_{u1}) \chi_i^u = \sum_{u=1}^{h} k_{ub} \chi_i^u - \psi_1^b \sum_{u=1}^{h} k_{u1} \chi_i^u$$
$$= 0 .$$

This identity, by (3), (5) and (6), reduces to

$$- \psi_1^b + \varepsilon \chi_i^a = 0 .$$

Now reference to (1) shows that (7) holds when $i = 1$, so that in particular,

$$- \psi_1^b + \varepsilon \chi_1^a = 0 .$$

Therefore

$$\chi_i^a = \chi_1^a \qquad (a > 1) ,$$

for each permutation of degree n . Since χ_1^a is the degree of an irreducible representation of G (not the identical representation), the characteristic of every substitution in that constituent which corresponds to a permutation of degree n is the sum of χ_1^a units, that is, each such substitution is the identity. Then this irreducible representation is isomorphic to a quotient group of G , and G has an invariant subgroup in which are included all its permutations of degree n .

A subgroup is called a *characteristic subgroup* if it is invariant in the holomorph of the group in which it occurs.

II. In a group of degree n and class $n-1$ the permutations of degree n constitute, with the identity, a characteristic subgroup.

The $n-1$ permutations of degree n in a transitive group of degree n and class $n-1$ generate an invariant subgroup (H) of G. Now H is transitive if G is transitive, for in an intransitive group of degree n and class $n-1$ the number of permutations of degree n is less than $n-1$ (§ 11, IV). In fact, such an intransitive group has just one transitive constituent of degree n' ($< n$) and of class $n'-1$, to which one or more regular groups in other letters are isomorphic. Thus proof of our theorem is required only when G is transitive. If the transitive subgroup H is of class $n-1$, it has, by I, an invariant subgroup H', generated by the permutations of degree n of G. This is absurd, as H was generated by those substitutions. Since G has but one subgroup of degree and order n, that subgroup is a characteristic subgroup.

An Abelian group whose order is a power of a prime number p, and in which no substitution is of order p^2, is called an *elementary group.*

III. If a transitive group of degree n and class $n-1$ is primitive, n is a power of a prime number, and the characteristic subgroup of order n is an elementary group.

As before, let G be the given primitive group of degree n and order g, and let H be its characteristic subgroup of order n. Let G' be a subgroup (of order g/n) that leaves fixed one letter of G. A Sylow subgroup of H is also a Sylow subgroup of G. Let P be a Sylow subgroup of order p^m. Then the largest subgroup (I) of G in which P is invariant is of order gn'/n, if n' is the order of the largest subgroup of H in which P is invariant. Hence I contains a maximal subgroup G' of G and therefore coincides with G; and P coincides with H. The invariant permutations (§ 9, II) of order p of H constitute (with the identity) a characteristic subgroup (K) of P. Hence K is an invariant subgroup of G, $\{K, G'\}$ is G, and

$$K = P = H.$$

§ 33.

The Reduction of Transitive Groups.

If g_1' is the number of substitutions of G' that are conjugate to S_1 under G, (6) of § 31 becomes, for $w = 1$,

$$(1) \qquad \sum_{u=1}^{h} k_{u1}\chi_1^u = \frac{gg_1'}{g'g_1}.$$

Now let G be a transitive permutation group of degree n, and let G' be a subgroup that leaves one letter fixed. Let χ_i be the characteristic of S_i for G. It is the number of letters of G that S_i does not displace. Then

$$ng'_i/\chi_i = g_i ,$$

so that

$$\sum_{u=1}^{h} k_{u1}\chi_i^u = \chi_i \qquad (i = 1, 2, \cdots, g) . \tag{2}$$

Stated in words, this is:

I. The number of times that a given irreducible representation Γ_u *occurs (with characteristics in the same sequence) when a transitive permutation group G is completely reduced, is equal to the number of linearly independent invariants of the first degree in* Γ'_u*, the subgroup of* Γ_u *that corresponds to the subgroup of G that fixes one letter.*

If G' permutes the n letters of G in m transitive constituents (counting constituents of one letter), we can show that

$$\sum_{u=1}^{h} k_{u1}^2 = m . \tag{3}$$

From (5) of § 31,

$$g'k_{u1} = \sum_{i=1}^{g'} \chi_i^u .$$

Multiply by k_{u1} and sum,

$$\begin{aligned} g' \sum_{u=1}^{h} k_{u1}^2 &= \sum_{i=1}^{g'} \sum_{u=1}^{h} k_{u1}\chi_i^u \\ &= \sum_{i=1}^{g'} \chi_i , \\ &= g'm . \end{aligned}$$

For a doubly transitive group $m = 2$, so that such a group has, when reduced, an irreducible constituent of degree $n - 1$ whose characteristics are integers, $\chi_i - 1$. For a simply transitive non-regular group, $m \geqq 3$ (§ 17). If $k_{u1} = 0$ $(u \geqq 3)$, then $k_{21} > 1$, and since $\chi_i = 0$ if S is of degree n in G, § 31, (6) reduces to

$$1 + k_{21}\chi_i^{(2)} = 0 .$$

But this is impossible because $\chi_i^{(2)}$ is an algebraic integer. Therefore (cf. § 30):

II. When a simply transitive group of order > 2 is completely reduced, at least three dissimilar irreducible representations occur.

§ 34.

Groups of Degree n Containing a Circular Permutation of n Letters.

I. If a simply transitive non-cyclic group of degree p^m contains a circular permutation of p^m letters, it has an invariant subgroup.

The characteristic equation of the permutation

$$S = (x_0 x_1 \cdots x_{n-1})$$

is

$$t^n - 1 = 0,$$

so that S is of variety n, when the group G in which it occurs is of degree n. Corresponding substitutions of similar groups have the same characteristic equation. Then no two irreducible constituents of G are similar groups. Let G' be the subgroup of G that leaves x_0 fixed. The subgroup of any irreducible constituent of G that corresponds to G' has one and only one linear invariant (§ 33).

Let ω be a primitive n^{th} root of unity. There is one and only one linear function of $x_0, x_1, \cdots, x_{n-1}$ which S transforms into ω^i times itself:

$$y_i = \sum_{j=0}^{n-1} \omega^{-ij} x_j \qquad (i = 0, 1, \cdots, n-1).$$

These n equations define a substitution T of non-zero determinant which transforms S into the canonical form:

$$y_i = \omega^i y_i' \qquad (i = 0, 1, \cdots, n-1).$$

The inverse of T is

$$n x_j = \sum_{i=0}^{n-1} \omega^{ij} y_i \qquad (j = 0, 1, \cdots, n-1).$$

It is possible to completely reduce G, and then transform each constituent in such a way that S goes into the canonical form. Then the substitution T, followed by a certain permutation of the subscripts of the new variables, completely reduces G.

We assume that G has no invariant subgroup. Hence no irreducible representation of G, except the identical one, is on one variable. In every irreducible representation (of degree $\geqq 2$) the substitution S is of order n. Now the coefficients of $T^{-1}GT$ are rational functions of ω, and if ω is replaced by any other primitive n^{th} root of unity, as ω_1, a given irreducible constituent of G is either unaltered thereby, or becomes another irreducible constituent of G. But when ω is replaced by ω_1, the s given multipliers of S in a certain irreducible constituent go over into the s multipliers of S in the same or another irreducible constituent. Consequently the $\varphi(n)$ primitive roots of unity, multipliers of S, are evenly distributed among t irreducible constituents of degree s each.

Let $x_{b_1}, x_{b_2}, \cdots, x_{b_r}$ $(r < n - 1)$ be the letters of a transitive constituent of G'. Both x_0 and $x_{b_1} + x_{b_2} + \cdots + x_{b_r}$ are linear invariants of G'. The substitution T transforms them into

$$\sum_{i=0}^{n-1} y_i/n$$

and

$$\sum_{i=0}^{n-1} y_i \sum_{v=1}^{r} \omega^{ib_v}/n .$$

Let $y_{a_1}, y_{a_2}, \cdots, y_{a_s}$ $(s < n - 1)$ be the variables of some irreducible constituent Γ of G. Then

$$\sum_{u=1}^{s} y_{a_u}$$

and

$$\sum_{u=1}^{s} y_{a_u} \sum_{v=1}^{r} \omega^{a_u b_v} .$$

are both invariants of the subgroup Γ' of Γ that corresponds to G'. But Γ' has only one linear invariant. Therefore

$$(1) \qquad \sum_{v=1}^{r} \omega^{a_1 b_v} = \sum_{v=1}^{r} \omega^{a_2 b_v} = \cdots = \sum_{v=1}^{r} \omega^{a_s b_v} .$$

If $n = p^m$, S has at least one primitive n^{th} root of unity among its multipliers in every irreducible constituent group of G. That is,

$$ts = p^m - 1 .$$

Let $n = p^m$ $(m > 1, p \text{ a prime})$. We are at liberty to assume that $\omega^{a_1} = \vartheta$ is a primitive n^{th} root of unity and that $\omega^{a_2} = \alpha$ is a primitive p^{th} root of unity. If we put

$$b_v = c_v p^{m-1} + d_v , \qquad d_v < p^{m-1} \qquad (v = 1, 2, \cdots, r) ,$$

and

$$\vartheta^{p^{m-1}} = \alpha^k ,$$

(1) gives

$$(2) \qquad \sum_{v=1}^{r} \vartheta^{d_v} \alpha^{kc_v} - \sum_{v=1}^{r} \alpha^{d_v} = 0 .$$

Not every $b_1, b_2, \cdots, b_r$ is congruent to zero, modulo p, because

$$\sum_{v=1}^{r} \vartheta^{b_v} \neq r .$$

The equation

$$(3)\qquad x^{p^{m-1}(p-1)} + x^{p^{m-1}(p-2)} + \cdots + x^{p^{m-1}} + 1 = 0$$

is known to be irreducible, not merely in the field of rational numbers, but also when to the rational field are adjoined any roots of unity whose orders are relatively prime to p. Hence, if in (2) the coefficients of every power of ϑ (and of α) are not zero, (2) is a multiple of

$$\alpha^{p-1} + \alpha^{p-2} + \cdots + \alpha + 1 .$$

In either event the p coefficients of the p powers of α are equal.

Now assume that just e exponents c_v are zero, and that f exponents d_v are congruent to zero, modulo p:

$$c_1 = c_2 = \cdots = c_e = 0 \qquad (0 \leqq e \leqq r),$$

$$d_1 \equiv d_2 \equiv \cdots \equiv d_f \equiv 0, \text{ mod } p \qquad (0 \leqq f < r).$$

Comparing the coefficients of powers of α in (2),

$$\begin{aligned}\sum_{v=1}^{e} \vartheta^{d_v} - f &= \sum_{v=e+1}^{e'} \vartheta^{d_v} - f' \\ &= \sum_{v=e'+1}^{e''} \vartheta^{d_v} - f'' \\ &= \cdots\cdots\cdots .\end{aligned}$$

If $e = r$, ϑ is a root of the equation

$$\sum_{v=1}^{r} x^{d_v} = f - f',$$

the degree of which is less than p^{m-1}, that is, is less than the degree of (3). If $e < r$, the exponents $d_{e+1}, d_{e+2}, \cdots, d_{e'}, d_{e'+1}, d_{e'+2}, \cdots, d_{e''}, \cdots,$ must be $d_1, d_2, \cdots, d_e$ over again, and therefore

$$f = f' = f'' = \cdots = f^{(p-1)} .$$

Then

$$r \equiv 0, \text{ mod } p .$$

But $x_{b_1}, x_{b_2} \cdots, x_{b_r}$ is any transitive constituent (except x_0) of G'. This leads to the false conclusion that

$$n - 1 \equiv 0, \text{ mod } p .$$

Let n be an odd prime p. Then without the assumption that G is simple,

$$ts = p - 1,$$

and we can prove that G (of order $> p$) contains a characteristic subgroup of order p.

Consider a substitution Q of G whose order q is not divisible by q (q is not necessarily a prime). Let its characteristic in a certain irreducible constituent group of G be ψ. Now ψ, the sum of q^{th} roots of unity, is a rational function of ω, only if it is a rational number. Since ψ is independent of ω, Q has the same characteristic in every irreducible constituent group of G. But ψ is more than a rational number; it is a rational integer, because any sum of roots of unity is an algebraic integer.

The characteristic of Q in G is $1 + t\psi$; it is also the number of letters of G left fixed by Q. This is not zero, for G has at least two constituent groups (§ 34, II), so that $-1/t$ is not an algebraic integer. Let m_ψ be the number of permutations of G which fix $1 + t\psi$ letters. Let m be the number of permutations of G whose characteristic in the given irreducible representation is χ_s (the characteristic of S). The sum of the characteristics (§ 25) of all the substitutions of this irreducible constituent is

$$-m + m_1 + 2m_2 + \cdots + sm_s = 0. \tag{4}$$

In the same way (2) of § 29, which we may write

$$\sum_{i=1}^{g} \chi_i \bar{\chi}'_i = 0 \qquad (\chi_i \neq \bar{\chi}'_i), \tag{5}$$

can be applied to two irreducible constituent groups of G. Now

$$\sum (\omega^{a_1} + \omega^{a_2} + \cdots + \omega^{a_s})(\omega^{-ka_1} + \omega^{-ka_2} + \cdots + \omega^{-ka_s}),$$

where the summation extends to the $(p-1)/s$ substitutions of order p which are powers of S and have different characteristics, is, because of (5), a rational integer and is therefore $-s$. Hence (5) becomes

$$-ms + m_1 + 2^2m_2 + \cdots + s^2m_s = 0. \tag{6}$$

After elimination of m from (4) and (6),

$$s(m_1 + 2m_2 + \cdots + sm_s) = m_1 + 2^2m_2 + \cdots + s^2m_s.$$

Therefore

$$m_1 = m_2 = \cdots = m_{s-1} = 0 .$$

The group G, when n is an odd prime, is of class $n - 1$, and from § 32, III, it has a characteristic subgroup of order p. Hence the theorem:

II. A simply transitive non-cyclic group of degree p contains a characteristic subgroup of order p.

§ 35.

Groups of Order $p^\alpha q^\beta$.

Three general theorems will lead easily to the proof that no group of order $p^\alpha q^\beta$ (p and q being prime numbers) is simple.

I. For any irreducible group, $g_i\chi_i/\chi_1$ is an algebraic integer.

From § 25, (2), we have

$$X_iX_j = \sum_{k=1}^{h} c_{ijk}X_k ,$$

if X_i is put for $g_i\chi_i/\chi_1$. For a given subscript i, these equations become

$$(c_{i11} - X_i)X_1 + c_{i12}X_2 + c_{i13}X_3 + \cdots + c_{i1h}X_h = 0 ,$$

$$c_{i21}X_1 + (c_{i22} - X_i)X_2 + c_{i23}X_3 + \cdots + c_{i2h}X_h = 0 ,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$c_{ih1}X_1 + c_{ih2}X_2 + c_{ih3}X_3 + \cdots + (c_{ihh} - X_i)X_h = 0 .$$

Hence X_i is a solution of the equation

$$\begin{vmatrix} c_{i11} - t , & c_{i12} , & \cdots c_{i1h} , \\ c_{i21} , & c_{i22} - t , & \cdots c_{i2h} , \\ \cdots & \cdots & \cdots , \\ c_{ih1} , & c_{ih2} , & \cdots c_{ihh} - t , \end{vmatrix} = 0 .$$

We may remark in passing that

II. The order of an irreducible group is divisible by its degree.

For if (3) of § 29 is divided by χ_1, the degree of the group,

$$\sum_{i=1}^{h} \frac{g_i\chi_i}{\chi_1}\bar{\chi}_i = \frac{g}{\chi_1}.$$

Then, by Theorem I, g/χ_1 is an algebraic integer, and therefore a natural number.

III. If the degree ($\geqq 2$) *of an irreducible simple group is relatively prime to the number* ($\geqq 2$) *of substitutions in some complete set of conjugates, the characteristic of the set is zero.*

Let S be a substitution of order s of the i^{th} conjugate set of the irreducible group G of degree χ_1. If the characteristic of S is

$$\chi_i = \omega^{a_1} + \omega^{a_2} + \cdots,$$

where ω is a primitive s^{th} root of unity, the characteristic of S^n is

$$\chi_{i(n)} = \omega^{na_1} + \omega^{na_2} + \cdots.$$

Consider the product

$$\alpha = (g_i/\chi_1)^{\phi(s)} \prod_n \chi_{i(n)},$$

in which n runs through the $\varphi(s)$ positive integers less than and prime to s. The factor $\prod_n \chi_{i(n)}$ is a symmetric function of the $\varphi(s)$ primitive s^{th} roots of unity, and therefore is a rational integer. But α is an algebraic integer (by I) and hence it too is a rational integer. Now

$$\prod_n \chi_{i(n)} = \operatorname{mod} \prod_n \chi_{i(n)} = \prod_n \operatorname{mod} \chi_{i(n)},$$

so that $(g_i/\chi_1)^{\phi(s)} \prod_n \operatorname{mod} \chi_{i(n)}$ is a rational integer. If g_i and χ_1 are relatively prime, $\prod_n \operatorname{mod} \chi_{i(n)}$ is zero or divisible by $\chi_1^{\phi(s)}$. Since $\chi_{i(n)}$ is a sum of χ_1 roots of unity, the largest value that mod $\chi_{i(n)}/\chi_1$ can have is unity, and this value is realized only when the χ_1 multipliers of S^n are equal. Only the identity has χ_1 for its characteristic. Then S^n is invariant in G. But G is a simple group of composite order. Finally, χ_i is zero if g_i ($\geqq 2$) is relatively prime to χ_1.

IV. In no simple group is the number of substitutions in some conjugate set a power of a prime.

If the given group G (of order g) is written as a regular group and is completely reduced,

$$\sum_{j=1}^{h} (\chi_1^j)^2 = g.$$

Now $\chi_1^1 = 1$, and g is divisible by $g_i = p^m$, a power of a prime. Therefore there is at least one irreducible representation whose degree χ_1 is not divisible by p, and in it, χ_i is zero or else $(\chi_1 > 1)$ all the substitutions of the i^{th} set are similarity substitutions, that is, are invariant in G. If $\chi_1 = 1$, G has an invariant subgroup with respect to which the quotient group is Abelian. If χ_i is zero in every irreducible representation of degree greater than unity and relatively prime to p,

$$\sum_{j=1}^{h} \chi_1^j \chi_i^j = 0,$$

of § 30, becomes

$$1 + p\beta = 0,$$

where β is an algebraic integer.

V. A group whose order is divisible by two and only two distinct primes has an invariant subgroup.

If $g = p^\alpha q^\beta$, an invariant substitution of a subgroup of order q^β belongs to a set in which the number of conjugate substitutions is p^m.

CHAPTER V.

TRANSITIVE GROUPS.

§ 36.

The Largest Subgroup in Which a Given Subgroup or Permutation Is Invariant.

With this chapter we take up once more the direct study of groups of permutations. The proofs of the theorems now to be considered are in general longer and more involved than any that have been encountered in the preceding pages.

I. Let G_1 *be the subgroup that fixes one of the* n *letters of a transitive group* G. *Let* H *be a subgroup (permutation) of* G_1 *of degree* $n - m$ $(0 < m < n)$ *and let* I *be the largest subgroup of* G *in which* H *is invariant. Then* I *has as many transitive constituents in the* m *letters fixed by* H *as there are different conjugate sets in* G_1 *which, under the permutations of* G, *enter into the complete set of conjugates to which* H *belongs. The degree of each of these constituents is proportional to the number of subgroups (permutations) in the several conjugate sets of* G_1 *in question.*

Let g be the order of G, and let those conjugates of H, which are found in G_1, lie in k different sets, in so far as they are permuted by the permutations of G_1 only, with r conjugates in the set that includes H, r_1 in a second set, and so on. In G_1, H is invariant in a subgroup of order g/nr, while H_1, a subgroup (permutation) in the second set, is invariant in a group of order g/nr_1. The largest subgroup I of G in which H is invariant is of order gm/ns $(s = r + r_1 + \cdots + r_{k-1})$. Now I does not connect transitively the $n - m$ letters displaced by H and the m letters it leaves fixed. Since the largest subgroup of G_1 in which H is invariant is of order g/nr, I has one transitive constituent of degree

$$(gm/ns)/(g/nr) = mr/s$$

in letters left fixed by H (§ 11, IV). Let $a_1, a_2, \cdots, b_1, b_2, \cdots$ be the letters of G left fixed by H. The letter fixed by G_1 is a_1. Consider a permutation $S = (a_1 b_1 \cdots) \cdots$ of G. Since there are permutations of G which transform H_1 into H we may assume that S transforms H_1 into H.

Then

$$SHS^{-1} = H_1 ,$$

$$(G_1S)H(G_1S)^{-1} = G_1H_1G_1^{-1} = H_1' ,$$

that is, every permutation $G_1S = (a_1b_1 \cdots) \cdots$ of G transforms some subgroup (permutation) H_1' (conjugate to H_1 under permutations of G_1) into H:

$$(G_1S)^{-1}H_1'(G_1S) = H .$$

Then no matter by which of the permutations $(a_1b_1 \cdots) \cdots$ of G we transform G_1 we get a group G_2 that fixes b_1 and in which H is a member of that set of r_1 conjugates by which every permutation $G_1S = (a_1b_1 \cdots) \cdots$ replaces the set $H_1 , \cdots$ of G_1. Then b_1 is one of the letters of a transitive constituent of degree mr_1/s in I. Since no permutation $(a_1b_1 \cdots) \cdots$ transforms H into itself, the letter a_1 is not an element of this transitive constituent in the mr_1/s letters $b_1 , b_2 , \cdots$. If mr_1/s is not unity, there is a permutation $T_2 = (b_1b_2 \cdots) \cdots$ in I, and the product $ST_2 = (a_1b_2 \cdots) \cdots$ transforms H_1 into H, as do also the products $ST_3 = (a_1b_3 \cdots) \cdots , \cdots$, where $T_3 = (b_1b_3 \cdots) \cdots , \cdots$. Every permutation G_1ST_i $(i = 2 , 3 , \cdots)$ transforms some subgroup (permutation) H_1' (conjugate of H_1 in G_1) into H. Suppose that a permutation $S_1 = (a_1c_1 \cdots) \cdots$ transforms H_1 into H. Then $S^{-1} = (b_1a_1 \cdots) \cdots$ transforms H into H_1, so that $S^{-1}S_1 = (b_1c_1 \cdots) \cdots$ transforms H into itself, thereby showing that c_1 is one of the above letters $b_1 , b_2 , \cdots$. If S_1 had transformed H_1' (some other member of the set $H_1 , \cdots$ of G_1) into H, a properly chosen permutation $G_1S_1 = (a_1c_1 \cdots) \cdots$ would have transformed H_1 into H, and that permutation could have been called S_1. Then no permutation $(a_1c_1 \cdots) \cdots$ (c_1 not one of the letters $b_1 , \cdots$) can transform any member of the set $H_1 , \cdots$ into H. Next, there must be a permutation in G to transform H_2 into H: call it $U = (a_1c_1 \cdots) \cdots$. We know that c_1 does not belong to the same transitive constituent in I as a_1 or b_1. Then just as before I has a transitive constituent in the mr_2/s letters $c_1 , c_2 , \cdots$ associated with the conjugate set $H_2 , \cdots$ of G_1. Thus we find $k - 1$ transitive constituents in r_1m/s letters $b_1 , b_2 , \cdots$, in r_2m/s letters $c_1 , c_2 , \cdots$, in r_3m/s letters $d_1 , d_2 , \cdots$, and so on, associated with the $k - 1$ conjugate sets $H_1 , \cdots , H_2 , \cdots , H_3 , \cdots , \cdots$ of G_1, in addition to the constituent of degree rm/s in the letters $a_1 , a_2 , \cdots$. Every permutation $(a_1a_2 \cdots) \cdots , (a_1a_3 \cdots) \cdots , \cdots$ transforms some subgroup (permutation) H' (of the set $H , \cdots$ of G_1) into H.

§ 37.

The Transitive Constituents of the Subgroup That Fixes One Letter of a Uniprimitive Group.

All multiply transitive groups are primitive. Simply transitive groups may be primitive or imprimitive. We shall for the sake of brevity call simply transitive primitive groups, *uniprimitive groups.* The subgroup that leaves one letter of a uniprimitive group fixed is intransitive and of degree $n - 1$ (§ 17).

I. A prime that divides the order of the subgroup that fixes one letter of a uniprimitive group, divides the order of every constituent group of that subgroup.

Let G_1 be a subgroup that fixes one letter of a uniprimitive group G of degree n. If the order of G_1 is divisible by a prime p that does not divide the order of every transitive constituent group of G_1, the subgroup H, generated by all the permutations of order p of G_1, is invariant in G_1 and displaces no letter of any transitive constituent of G_1 whose order is not divisible by p. Since G is transitive, H is not invariant in G, and since G is primitive, G_1 is a maximal subgroup of G and is therefore the largest subgroup of G that transforms H into itself. Then by § 36, since H fixes certain letters of G_1, there should be other subgroups in G_1, conjugate to H under G. But since H contains all the permutations of order p of G_1, and is generated by them, this is impossible. Then p divides the order of every constituent of G_1.

II. Let G_1 be the subgroup that fixes one letter of a uniprimitive group. If one constituent of G_1 is a regular group of order p^n (p a prime), G_1 is of order p^n.

Since one transitive constituent (A) of G_1 is of order p^n, G_1 is of order p^m ($> p^n$, say). Then G_1 has an invariant subgroup H of order p^{m-n} (§ 11) whose permutations displace no letter of A. By § 36, because of H and the one letter of G fixed by G_1, G_1 must have p^n conjugate subgroups similar to H. But (§ 10, V, VI) no group of order p^m has so many as p^n subgroups of order p^{m-n} in one complete set of conjugates.

§ 38.

Multiply Transitive Constituents of the Subgroup That Fixes One Letter of a Uniprimitive Group.

I. Let G_1, the subgroup that fixes one letter of a uniprimitive group G of degree n and order g, have a multiply transitive constituent of degree m. If G_1 has no transitive constituent whose degree is a divisor

($> m$) of $m\ (m-1)$, all the transitive constituents of G_1 are isomorphic multiply transitive groups of degree m and order g/n.

Let $G(x)$ be the subgroup (G_1) that leaves the letter x fixed. Let $a_1, a_2, \cdots, a_m$ be the letters of the given (at least) doubly transitive constituent (A) of degree m of $G(x)$. The order of $G(x)$ is g/n, that of $G(x)(a_1)$ (fixing first x and then a_1) is $g/(nm)$, and that of $G(x)(a_1)(a_2)$ is $g/[nm(m-1)]$. Obviously

$$G(x)(a_1) = G(a_1)(x)\,.$$

The subgroup $G(x)(a_1)$ has a transitive constituent of degree $m-1$ in the letters $a_2, a_3, \cdots, a_m$. In the subgroup $G(a_1)$, x is a letter of a transitive constituent of degree m. If in $G(a_1)$ the letters $a_2, a_3, \cdots, a_m$ form a transitive constituent of degree $m-1$, or if they form with x a transitive constituent of degree m, $G(x)$ is not a maximal subgroup of G. If the transitive constituent $a_2, a_3, \cdots, a_m, \cdots$, of $G(a_1)$ is of degree μ ($\geqq m$), $G(a_1)(a_2)$ is of order $g/(n\mu)$; and if δ is the degree of the transitive constituent of $G(a_1)(a_2)$ in which x is included,

$$g/(n\mu\delta) = g/[nm(m-1)]\,.$$

Since by hypothesis μ (when $\mu > m$) does not divide $m(m-1)$, $\mu = m$. The constituent $c_1, a_2, a_3, \cdots, a_m$ in $G(a_1)$, because it has a transitive subgroup of degree $m-1$, is doubly transitive.

Since the order of $G(a_1)(a_2)$ is $g/(nm)$, x is in a transitive constituent of degree $m-1$ of $G(a_1)(a_2)$ and therefore is in a doubly transitive constituent of degree m of $G(a_1)$. If

$$x,\ b'_2,\ b'_3,\ \cdots,\ b'_m \text{ and } c_1,\ a_2,\ a_3,\ \cdots,\ a_m$$

are the letters of the two doubly transitive constituents of $G(a_1)$ that have been mentioned, the permutations of $G(x)$ which transform $G(a_1)$ into $G(a_2)$ replace the letters of these constituents of $G(a_1)$ by

$$x,\ b''_2,\ b''_3,\ \cdots,\ b''_m \quad \text{and } c_2,\ a_1,\ a_3,\ \cdots,\ a_m\,.$$

Similarly the two corresponding constituents of $G(a_3)$ are

$$x,\ b^3_2,\ b^3_3,\ \cdots,\ b^3_m \text{ and } c_m,\ a_1,\ a_2,\ \cdots,\ a_{m-1}\,.$$

. . . .

Finally when $G(a_1)$ is transformed into $G(a_m)$, we get

$$x,\ b^m_2,\ b^m_3,\ \cdots,\ b^m_m \text{ and } c_m,\ a_1,\ a_2,\ \cdots,\ a_{m-1}\,.$$

If $c_1 = c_2$, say,

$$\{G(a_1)\,,\,G(a_2)\} = G$$

permutes the letters $c_1, a_1, a_2, \cdots, a_m$ among themselves. Then $G(x)$ has a transitive constituent C on the m letters $c_1, c_2, \cdots, c_m$, which is, moreover, doubly transitive, because

$$G(x)(c_1) = G(x)(a_1)$$

has a permutation that replaces c_2 by c_1 at the same time that it replaces a_2 by a_i $(i = 3, 4, \cdots, m)$. Of course, C and A are homomorphic (§ 11) but since $G(x)(c_1)$ and $G(x)(a_1)$ are identical, C and A are isomorphic.

The $m(m-1)$ letters $b'_2, b'_3, \cdots, b'_m, b''_2, \cdots, b^m_m$ are permuted transitively by $G(x)$ so that if there are repetitions among them one letter occurs as often as any other, ϱ times, say. Hence there is in $G(x)$ a transitive constituent of degree $m(m-1)/\varrho = m$. Now the letters $b_1, b_2, \ldots, b_m$ (dropping accents in $G(a_1)$ and calling the m^{th} letter b_1) are permuted as a doubly transitive constituent of $G(x)$. This follows from the fact that the letters $x, b'_2, b'_3, \cdots, b'_m$ and $x, b''_2, b''_3, \cdots, b''_m$, say, are not all the same, but each omits one of the letters $b_1, b_2, \cdots, b_m$, although all these letters are displaced by each group $G(a_1), G(a_2), \cdots, G(a_m)$. The sets $b'_i, b''_i, \cdots, b^m_i$ $(i = 2, 3, \cdots, m)$ are permuted according to the doubly transitive constituent A of $G(x)$ and therefore the letters $b_1, b_2, \cdots, b_m$ which serve to characterize these m sets belong to a doubly transitive constituent B of $G(x)$. Since

$$G(x)(a_1) = G(x)(b_1)\,,$$

B is isomorphic to A. If B coincides with C,

$$\{G(x)\,,\,G(a_1)\} = G$$

is of degree $2m+1$ and the theorem is true as stated.

Then assume that $n > 2m+1$. Since the $m-1$ letters $c_2, c_3, \cdots, c_m$ are the letters of a transitive constituent of

$$G(x)(c_1) = G(a_1)(x)\,,$$

$G(a_1)$ has a transitive constituent $d_1, c_2, c_3, \cdots, c_m, \cdots$ whose degree divides $m(m-1)$ and is therefore m. As before, transformation of $G(a_1)$ by permutations of $G(x)$ reveals a fourth doubly transitive constituent D isomorphic to A in $G(x)$ unless $d_1 = d_2$ (say), or unless the constituents D and B coincide. If $d_1 = d_2$, G is intransitive. If D and B coincide,

$$\{G(x)\,,\,G(a_1)\} = G$$

is of degree $3m+1$, and the theorem is true. Evidently the theorem can be proved by induction.

Let it be assumed that $G(x)$ has exactly k ($\geqq 3$) isomorphic doubly transitive constituents of degree m: $A, B, \cdots, K$, on the letters

$$a_1, a_2, \cdots, a_m;$$
$$b_1, b_2, \cdots, b_m;$$
$$\cdots\cdots\cdots\cdots$$
$$k_1, k_2, \cdots, k_m;$$

respectively. The $k-1$ transitive constituents of $G(a_1)$ on the letters

$$x, b_2, b_3, \cdots, b_m;$$
$$c_1, a_2, a_3, \cdots, a_m;$$
$$d_1, c_2, c_3, \cdots, c_m;$$
$$\cdots\cdots$$
$$k_1, j_2, j_3, \cdots, j_m;$$

are doubly transitive groups. It is also assumed that

$$G(x)(a_1) = G(x)(b_1) = G(x)(c_1) = \cdots = G(x)(k_1).$$

Another transitive constituent of $G(a_1)$ is on the μ letters

$$l_1, k_2, k_3, \cdots, k_m, \cdots.$$

Since

$$G(a_1)(k_2)(x) = G(x)(a_1)(k_2) = G(x)(k_1)(k_2),$$
$$\mu = m(m-1)/\delta = m.$$

The permutations of $G(x)$ that transform $G(a_1)$ into $G(a_2)$, $G(a_3)$, $\cdots$, $G(a_m)$, replace

$$l_1, k_2, k_3, \cdots, k_m;$$

by

$$l_2, k_1, k_3, \cdots, k_m;$$
$$\cdots\cdots$$
$$l_m, k_1, k_2, \cdots, k_{m-1};$$

respectively. If $l_1 = l_2$,

$$\{G(a_1), G(a_2)\} = G$$

has a transitive constituent of degree $(k-1)m+1$. Then the m distinct letters $l_1, l_2, \cdots, l_m$ belong to a doubly transitive constituent L of $G(x)$, isomorphic to A because

$$G(x)(l_1) = G(x)(a_1).$$

But since $G(x)$ has only k isomorphic doubly transitive constituents of degree m, L must coincide with one of the given constituents, and because of $G(a_1)$, the only constituent of $G(x)$ with which it can coincide is B. Then

$$\{G(x), G(a_1)\} = G$$

is of degree $km + 1$. Since the theorem is true when $k = 1, 2$, and 3, it is, by a complete induction, true in every case.

§ 39.

Invariant Subgroups of Primitive Groups.

I. An invariant subgroup of a t-ply transitive group is at least $t-1$ times transitive, if an exception is made of the elementary group of order 2^m that occurs in certain triply transitive groups.

The theorem is obvious and trivial in case $t = 1$.

Let G be a group of degree n that is t ($\geqq 2$) times transitive, and let H be an invariant subgroup of G. Let S be a permutation of H and let $C_1, C_2, \cdots, C_k$ ($k < n$) be its component circular permutations of one or more letters. Let $C_1, C_2, \cdots, C_r$ ($r \leqq k$) be so selected that, (1) $C_1C_2 \cdots C_r$ contains at least t letters, (2) if C_r (say) is omitted, $C_1C_2 \cdots C_{r-1}$ contains $t - s$ ($< t$) letters.

Assume for the moment that $s > 1$. Let $a_1, a_2, \cdots, a_t$ be the first letters of S as now arranged. A permutation T of G fixes $a_1, a_2, \cdots, a_{t-1}$ and replaces a_t by b.

$$T^{-1}ST = C_1C_2 \cdots C_{r-1} (\cdots a_{t-1}b \cdots) \cdots$$

is a permutation of H; so also is $S^{-1}T^{-1}ST = U$, which fixes $t-2$ of the $t-1$ letters $a_1, a_2, \cdots, a_{t-1}$, and replaces a_t by b. There is in G a permutation V that replaces a_t, b, and the $t-2$ letters $a_1, a_2, \cdots$ fixed by U, by t arbitrary letters $\alpha_1, \alpha_2, \cdots, \alpha_t$. Then $V^{-1}UV$ fixes the $t-2$ letters $\alpha_3, \alpha_4, \cdots, \alpha_t$ and replaces α_1 by α_2. Since H includes $V^{-1}UV$, it is at least $t-1$ times transitive.

It is very different if for every permutation S of H and for every arrangement of the component circular permutations of S, $C_1C_2 \cdots C_{r-1}$ is of degree $t-1$. Suppose that $C_1, C_2, \cdots, C_k$ are so given that the degree of C_1 is not less than that of C_2, the degree of C_2 is not less than that of C_3, and so on. Then unless C_1 and C_r displace the same number of letters,

$C_rC_2C_3 \cdots C_{r-1}C_1$ contains at least t letters and $C_rC_2C_3 \cdots C_{r-1}$ contains at most $t-2$ letters. Therefore the permutation S is regular, of degree n, and its order divides $t-1$. If H is intransitive, G is imprimitive and the theorem is true. If H is transitive, it is a regular group, and simply transitive. But H is $t-2$ times transitive, for, regarding G as a $t-1$ times transitive group, $C_1C_2 \cdots C_{r-1}$ is of degree $t-1$ and $C_1C_2 \cdots C_{r-2}$ is of degree less than $t-2$. Therefore $t=3$, and the order of every permutation of H divides 2. By § 7, III, H is an elementary group of order 2^m. An example is the symmetric group of degree 4, in which the subgroup

$$1, \quad (12)(34), \quad (13)(24), \quad (14)(23)$$

is invariant.

It follows almost immediately that

II. Alternating groups of degree $\geqq 5$ *are simple.*

Since alternating groups of degree n ($\geqq 5$) are $n-2$ times transitive, a self-conjugate subgroup of an alternating group is $n-3$ times transitive and therefore is of order $n!/6$. In the alternating group of degree n there are exactly $n!/[20(n-5)!]$ subgroups of degree and order 5. They constitute a single conjugate set and should therefore all be in the invariant subgroup of order $n!/6$. But in the latter there are exactly $n!/[5!(n-5)!]$ subgroups of degree and order 5.

§ 40.

Invariant Imprimitive Subgroups of Doubly Transitive Groups.

I. If a doubly transitive group has an invariant imprimitive subgroup, its degree is p^m *(*p *a prime) and the given subgroup is of class* p^m *or* p^m-1 *and includes an elementary group of order* p^m*, invariant in* G.

Let the doubly transitive group G of degree kq have an invariant subgroup H of order h; let G_1 and H_1 be the subgroups of G and H, respectively, that leave a letter a_1 fixed. One of the smallest systems of imprimitivity of H is composed of the q letters $a_1a_2 \cdots a_q$, say. Any permutation of G_1 transforms the system $a_1a_2 \cdots a_q$ into another system $a_1b_2 \cdots b_q$. Now if the two systems of imprimitivity have two or more but not all their letters in common it means that H has two subgroups of order h/k which have a cross-cut including H_1 of order greater than h/kq. Then the two or more common letters of the two systems are another system of imprimitivity of less than q letters, contrary to hypothesis. Because G_1 is transitive, every letter of G_1 is in a system of q letters with

a_1. Any permutation of H_1 permutes among themselves the $q-1$ letters of each of the systems that have a_1 in common. Suppose that a permutation S of H fixes both a_1 and a_2. There are in H two systems $b_2a_1\cdots$ and $b_2a_2\cdots$ which have only b_2 in common. Each of these two systems should be unchanged by $S=(a_1)(a_2)\cdots$. But S transforms them into $b_2a_1b_3\cdots$ and $b_2a_2b_3\cdots$, which have at least two letters in common. Now S fixes all the letters of H except $a_3, a_4, \cdots, a_q$. If the same reasoning is applied to $S=(a_1)(b_2)(a_3a_4\cdots)\cdots$ as was applied to $(a_1)(a_2)(b_2b_3\cdots)\cdots$, it follows that S is the identity and H is of class kq or $kq-1$. In either event G has an invariant subgroup E of order kq (§ 32) whose $kq-1$ permutations of degree kq form a complete set of conjugates under G. Then q is a prime (p) and the order of every permutation of E divides q. Since E is of order p^m, it has an invariant permutation of order p, which is transformed by G into an invariant permutation of E, and E is Abelian.

We have incidentally proved a theorem worth stating by itself:

II. If all the n letters of an imprimitive group are involved in $(n-1)/(q-1)$ systems of imprimitivity of q letters which have one letter in common, and if no two of these systems have more than the one letter in common, the imprimitive group is regular or of class $n-1$.

This suggests a similar theorem, to which we devote the next section. It, as well as II, will be required for the developments of § 47.

§ 41.

Certain Imprimitive Groups.

I. If all but q letters of an imprimitive group of degree n $(>2q)$ are involved in $(n-q-1)/(q-1)$ systems of imprimitivity of q letters which have one letter in common, and if no two of these systems have a second letter in common, H is regular or of class $n-1$.

Let $a_1a_2a_3\cdots a_q$, $a_1b_2b_3\cdots b_q$, $\cdots$ be the $(n-q-1)/(q-1)$ systems that have a_1 in common and in which every other letter of H except $\alpha_1, \alpha_2, \cdots, \alpha_q$ occurs once and once only. We shall call them the systems A. Any permutation S of H that fixes a_1 fixes each of the systems A. If $q=2$, S fixes every letter of A:

$$S=(\alpha_1\alpha_2),$$

and this is the only permutation of degree and order 2 in H. But $(\alpha_1\alpha_2)$ cannot be invariant in H, so that when $q=2$, H is a regular group. The theorem is to be proved in case $q \geqq 3$.

Any permutation of H that replaces a_1 by b_2 transforms the system $a_1b_2b_3 \cdots b_q$ into itself. Then $(a_1b_2 \cdots) \cdots$ replaces the systems A by systems B which have b_2 in common and no two of which have any other letter in common. Consider a permutation

$$S = (a_1)(b_2b_3 \cdots) \cdots .$$

If S fixes an additional letter x, it can be shown that x is not a letter of the systems B. For if x were a letter of B, the system $b_2x \cdots$ would contain b_3, so that the two systems $b_2a_1b_3 \cdots b_q$ and $b_2xb_3 \cdots$ of B would have two letters in common. Then S displaces all the letters of the system $a_1b_2b_3 \cdots b_q$ except a_1. It follows also that if S displaces a_2, it fixes no letter of A except a_1.

We wish to see if S can be of degree less than $n-1$. There are two cases to be examined: S may fix another letter of A or it may displace all the letters of A and fix α_1, say.

Let

$$S = (a_1)(a_2)(b_2b_3 \cdots) \cdots .$$

It displaces $b_4, b_5, \cdots, b_q$, and fixes $a_3, a_4, \cdots, a_q$. One of the systems B will contain a_2, and therefore also b_3, which is contrary to hypothesis, unless in every permutation $T = (a_1b_2 \cdots) \cdots$, $R = (a_1b_3 \cdots) \cdots, \cdots$ of H the letter a_2 is preceded by one of the letters α. In fact there must be two similar cycles $(a_1b_2b \cdots b)$ and $(\alpha\alpha \cdots \alpha a_2)$ in T. If now

$$T = (a_1b_2 \cdots)(a_2\alpha_2 \cdots) \cdots$$

and

$$R = (a_1b_3 \cdots)(a_2\alpha_2 \cdots) \cdots$$

$$TR^{-1} = (a_1b_i \cdots)(a_2) \cdots ,$$

which does not respect the system $a_1a_2 \cdots a_q$. Hence H contains $q-1$ permutations

$$(a_1b_i \cdots)(a_2\alpha_i \cdots) \cdots \qquad (i = 2, 3, \cdots, q).$$

Since S fixes a_3, and $q \geqq 3$, H contains the two permutations:

$$T = (a_1b_i \cdots)(a_2\alpha_i \cdots)(a_3\alpha \cdots) \cdots$$

and

$$U = (a_1b_j \cdots)(a_2\alpha_j \cdots)(a_3\alpha_i \cdots) \cdots .$$

But

$$TU^{-1} = (a_1b_k \cdots)(a_2a_3 \cdots) \cdots$$

is impossible. Then $S = (a_1)(b_2b_3\cdots)\cdots$ displaces all the letters of A except a_1.

Let

$$S = (a_1)(\alpha_1)(b_2b_3\cdots)\cdots.$$

At most one of the systems X into which a permutation $(a_1\alpha_1\cdots)\cdots$ transforms A is made up exclusively of letters α. Then since S fixes each of the systems X, as well as each of the systems A, one of the systems X contains at least two letters of one of the systems A. Let $\alpha_1a_2a_3\cdots$ be the transform of the system $a_1b_2b_3\cdots b_q$, say. It is not the transform of $a_1a_2\cdots a_q$. Any permutation $(\alpha_1a_2\cdots)\cdots$ transforms the system $\alpha_1a_2a_3\cdots$ into itself, and therefore the product

$$(a_1\alpha_1\cdots)\cdots(\alpha_1a_2\cdots)\cdots = (a_1a_2\cdots)\cdots$$

transforms the system $a_1b_2b_3\cdots b_q$ into $\alpha_1a_2a_3\cdots$. But $(a_1a_2\cdots)\cdots$, being a permutation of H, fixes the system $a_1a_2\cdots a_q$ and therefore cannot transform $a_1b_2b_3\cdots$ into $a_2a_3\alpha_1\cdots$.

No permutation $(\alpha_1\alpha_2\cdots)\cdots$ of H can fix all the $n-q$ letters of A, because certain systems of imprimitivity of q letters involve α_1 and some letters of A.

CHAPTER VI.

PRIMITIVE GROUPS WITH TRANSITIVE SUBGROUPS OF LOWER DEGREE.

§ 42.

Introduction.

I. A primitive group which contains a transitive subgroup of lower degree is doubly transitive.

In the primitive group G there is a subgroup H, transitive in the letters $a_1, a_2, \cdots, a_m$. Let $\alpha_1, \alpha_2, \cdots$, be the other letters of G. The theorem is true if $m = n - 1$ (§ 17). Let m be less than $n - 1$.

Because G is transitive, some permutation S of G replaces an a by an α. Of all such permutations let S displace a minimum number ($\geqq 1$) of letters α. But S does not displace more than $m - 1$ α's because the complete set of conjugate subgroups to which H belongs generates an invariant, and therefore transitive, subgroup of G, and the latter is generated by permutations of degree $\leqq m$, from which S might be selected. Thus S does not replace every a by an α. Suppose that S has a cycle made up entirely of α's. The transitive group $S^{-1}HS$ contains a permutation that replaces an a by an α and displaces none of the letters of the given cycle of S. Then S has no cycle of letters α alone. Hence $H' = \{H, S\}$ is a transitive group of degree $m + q$ $(0 < q < m)$. The letters $\alpha_1, \alpha_2, \cdots, \alpha_q$, if $q > 1$, are a system of imprimitivity of H'. Otherwise there is in H' a permutation T that replaces an α by an a and an α by an α, so that THT^{-1} contains a permutation that replaces an a by an α and displaces fewer than q α's. If $n = m + q$ $(q > 1)$, the permutation T can be taken from G and the same conclusion reached. Then $n > m + q$ if $q > 1$.

This process can be continued step by step until we have built up a transitive group K' of degree $m' + q' = n$. Now, as we have just seen, $q' = 1$, and G therefore is at least doubly transitive.

Incidentally we have proved that

II. A primitive group of degree n which contains a primitive subgroup of degree m is $n - m + 1$ times transitive.

For when H is primitive, $q = 1$, and H' is doubly transitive. If $m + 1 < n$, H'', formed from H' in the same way that H' was formed from H, is triply transitive, and so on, until finally a subgroup K of degree n is reached which is $n - m + 1$ times transitive.

§ 43.

The Transitive Subgroup.

Theorem II of the last section is only a special case of the following:

I. A primitive group of degree n which contains a transitive subgroup H of degree m ($< n$) is $n - m + 1$ times transitive unless H has $q + 1$ systems of imprimitivity of q letters which have one letter in common, and no two of which have a second letter in common.

If the primitive group in question is more than doubly transitive we can drop to one of its doubly transitive subgroups and prove the theorem for the latter. Then let G be a doubly (but not triply) transitive group of degree

$$m_r + 1 = m + q_1 + \cdots + q_r + 1 ,$$

in which are found transitive subgroups H, $H_1, \cdots, H_r$ of degree m, $m_1 = m + q_1, \cdots, m_r = m + q_1 + \cdots + q_r$, respectively. It is assumed that the degree of any transitive subgroup of G that displaces more than m and fewer than m_r letters is one of the numbers $m_1, m_2, \cdots, m_{r-1}$. This does not mean that there is no transitive subgroup of degree $< m$. Let $a_1, a_2, \cdots, a_m$ be the letters of H, and let $a^i_1, a^i_2, \cdots, a^i_{q_i}$ $(i = 1, 2, \cdots, r)$ be the letters displaced by H_i but not by H_{i-1} $(H_0 = H)$. Let F_i be the largest subgroup of G on the letters of H_i; F_i includes all the preceding subgroups F $(= F_0)$, $F_1, \cdots, F_{i-1}$, and is transitive.

In case $q_r = 1$, G is triply transitive, contrary to hypothesis; hence,

$$q_r > 1 .$$

It follows (see § 42, I) that $q_i > 1$ $(i = 1, 2, \cdots, r-1)$. If the letters $a^i_1, a^i_2, \cdots, a^i_{q_i}$ are not a system of imprimitivity in F_i, some permutation S of F_i will give a group $S^{-1}F_{i-1}S$ which displaces some of the letters $a^i_1, a^i_2, \cdots, a^i_{q_i}$ and fixes at least one of them. Then

$$\{F_{i-1} , S^{-1}F_{i-1}S\}$$

is a transitive group of degree $> m_{i-1}$ and $< m_i$ $(m_0 = q_0 = m)$, contrary to hypothesis. By the definition of imprimitivity all the subgroups of F_i, notably F, $F_1, \cdots, F_{i-1}$, admit these systems. In consequence the letters $a^x_1, a^x_2, \cdots, a^x_{q_x}$ fall into systems of imprimitivity q_i by q_i, for $x = 1, 2, \cdots, i-1$. Thus q_i divides q_{i-1}, but it is not yet clear that

$$q_i < q_{i-1} \; (i = 2, 3, \cdots, r) .$$

However, it was proved in § 42 that q_1 divides m and is $< m$.

Let a_{11}^r represent the system $a_1^r a_2^r \cdots a_{q_r}^r$ of F_r and let a_{1k}^i $(i=0, 1, \cdots, r-1; a^0=a; k=1, 2, \cdots, q_1/q_r)$ be the remaining systems into which a_{11}^r goes under transformation by the permutations of F_r. We define F_i' as the group according to which the systems $a_{11}, \cdots,$ of F_i are permuted. Since F_{r-1}' is transitive, F_r' is at least doubly transitive.

The group G displaces a letter b not in F_r, and, being doubly transitive, contains a permutation

$$T_k = (ba_k^r) \cdots \qquad (k=1, 2, \cdots, q_r).$$

Let it be granted for the moment that T_k transforms $F_{i+1}, F_{i+2}, \cdots, F_{r-1}$ each into itself and leaves fixed the letters $a_1^{i+1}, a_1^{i+2}, \cdots, a_1^{r-1}$. Then

$$\{T_k^{-1} F_i T_k, F_i\} = F_i;$$

for its degree is less than m_{i+1} and must consequently be m_i, the degree of F_i. If T_k displaces a_1^i, there is a permutation S in F_i which replaces a_1^i by the same letter as does T_k. Then $S^{-1}T_k$ leaves a_1^i fixed and may be used for T_k. But T_k transforms F_{r-1} into itself, and by multiplication by a permutation of F_{r-1}, a like permutation can be obtained, which leaves a_1^{r-1} fixed. Then by a complete induction G contains a permutation

$$T_k = (a_1)(a_1') \cdots (a_1^{r-1})(ba_k^r) \cdots \quad (k=1, 2, \cdots, q_r),$$

which transforms $F, F_1, \cdots, F_{r-1}$ each into itself. Each system of imprimitivity $a_1^i a_2^i \cdots a_{q_i}^i$ $(i < r)$ is transformed into itself. But the system a_{11} is replaced by q_r systems of imprimitivity which have at least the letter a_1 in common with a_{11}. Let these q_r new systems of F_{r-1} be represented by the symbol $a_{11}T_k$ $(k=1, 2, \cdots, q_r)$. If it be assumed that $a_{11}T_k$ has a second letter a_2 in common with a_{11},

$$T_k = (ba_k^r)(a_v a_2 \cdots)(a_1) \cdots,$$

where a_v is some letter of the system a_{11}. In F_r' there is a permutation

$$S = (a_{11}a_{11}^r)(b) \cdots$$

$$= \begin{pmatrix} a_1 & a_2 & a_v & a_k^r & b & & & \\ a_x^r & a_y^r & a_z^r & a_w & b & \cdot & \cdot & \cdot \end{pmatrix}.$$

Now

$$U = S^{-1}T_k S = (ba_w)(a_z^r a_y^r \cdots)(a_x^r) \cdots.$$

The transitive group

$$\{U^{-1}F_{r-1}U\,,\ F_{r-1}\}$$

omits a_y^r and a_x^r, and includes b; it is therefore of degree $> m_{r-1}$ and $< m_r$, contrary to hypothesis. We have proved then that the q_r systems $a_{11}T_k$ of F_{r-1} have one and only one letter in common with a_{11}, — the letter a_1.

Any permutation S of G that transforms F_i into itself generates with F_i a group which has a transitive constituent of degree m_i that admits $a_1^i a_2^i \cdots a_{q_i}^i$ as a system of imprimitivity. Otherwise

$$\{SF_{i-1}S^{-1}\,,\ F_{i-1}\}$$

is a transitive group of degree $> m_{i-1}$ and $< m_i$ $(i = 1\,,\ 2\,,\ \cdots,\ r)$.

Suppose it possible to find in G a permutation T that transforms F_{r-1} into itself, and which replaces the system a_{11} by a system α distinct from any one of those obtained by transforming F_{r-1} by T_k or by its own permutations. It may be assumed that T fixes a_1^{r-1}. For if it does not, it is only necessary to multiply T by a properly chosen permutation of F_{r-1}, which by hypothesis replaces α by a system α', not one of the $m_{r-1}(q_r + 1)/q_r$ known systems. It was shown that T_k transforms F_i into itself and fixes a_1^i $(i = 0\,,\ 1\,,\ \cdots,\ r - 1)$, and in the same way T can be chosen to leave F_i invariant and fix a_1^i $(i = 0\,,\ 1\,,\ \cdots,\ r - 1)$. Then T replaces b by a letter a_k^r, and permutes the rest of the letters $a_1^r a_2^r \cdots a_{q_r}^r$ among themselves. Now

$$TT_k^{-1} = (b)(a_1) \cdots = S\,,$$

is a permutation of F_r under which F_{r-1} is invariant. Hence S fixes the system a_{11},

$$T = ST_k\,,$$

and α is the system $a_{11}T_k$.

The system $a_{11}T_k$ bears the same relation to F_{r-1}, $T_k^{-1}F_rT_k$, and G, that a_{11} does to F_{r-1}, F_r, and G. From $a_{11}T_k$ then can be obtained, by means of permutations that leave a_1 fixed and F_{r-1} invariant, q_r other systems with but one letter in common with $a_{11}T_k$. But we have just seen that these q_r systems will coincide with systems already obtained. Hence the letters of F_{r-1} can be arranged in systems of imprimitivity of q_r letters each in at least $q_r + 1$ ways with one letter common to $q_r + 1$ systems and with no other letter common to any two of them. This result holds a fortiori for all transitive subgroups of F_{r-1} and in particular for H.

§ 44.

The Limit of Transitivity.

I. A primitive group of degree n which contains a transitive subgroup of degree m is at least $n - 2m + 3$ times transitive.

We continue the notation of § 43.

A primitive group of degree n that contains F_r is $n - m_r + 1$ times transitive. We know (§ 42) that $q_1 < m$, and if we can show that

$$(1) \qquad q_{i+1} < q_i \qquad (i = 1, 2, \cdots, r-1),$$

then, because q_{i+1} divides q_i and q_1 divides m,

$$\begin{aligned} m_r &\leqq m\left(1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^r}\right) \\ &\leqq 2m - m/2^r \\ &\leqq 2m - 2, \end{aligned}$$

and therefore

$$n - m_r + 1 \leqq n - 2m + 3.$$

The most important step towards the proof of (1) has been made. Since T_k permutes the letters $a_1, a_2, \cdots, a_{q_{r-1}}$ of a system of imprimitivity of F_{r-1} among themselves, the q_r^2 letters involved in systems a_{11}, $a_{11}T_1$, $\cdots$, $a_{11}T_{q_r}$ are all letters of the larger system $a_1a_2 \cdots a_{q_{r-1}}$. Then

$$(2) \qquad q_{r-1} \geqq q_r^2 > q_r.$$

Hence, if $m_r = m_1$, that is, if $r = 1$, the theorem is true.

It will now be shown that if F_r' is triply transitive, $r = 1$. Suppose that F_r' is triply transitive. To each of the $q_r + 1$ distinct arrangements of the letters of F_{r-1} in systems of imprimitivity of q_r letters with a_1 in common, there corresponds a doubly transitive group according to which the systems are permuted. Let $F_{r-1}(a_1)$ be the subgroup of F_{r-1} that fixes the letter a_1 (cf. § 38). The remaining $q_r - 1$ letters of each system of imprimitivity to which a_1 belongs are permuted only among themselves by the permutations of $F_{r-1}(a_1)$. Now $F_{r-1}'(a_{11})$ is transitive of degree $m_{r-1}/q_r - 1$, while the number of systems transitively connected by it cannot exceed $q_r - 1$. Hence $m_{r-1} \leqq q_r^2$, and since $q_{r-1} \geqq q_r^2$, $q_{r-1} = q_r^2$; in fact, $m_{r-1} = m = q_1^2$, and $r = 1$.

We now assume

$$r \geqq 2.$$

Is it possible for F_r' to have a transitive subgroup of degree $> m/q_r$ and not one of the numbers m_i/q_r? Let, if possible, F_{ik}' be a transitive subgroup of F'_{i+1} that displaces besides the letters of F'_i the k letters a^{i+1}_{11}, $a^{i+1}_{12}, \cdots, a^{i+1}_{1k}$ $(1 \leqq k < q_{i+1}/q_r;\ i=0, 1, \cdots, r-2)$. Then between F_i and F_{i+1} there is a corresponding subgroup F_{ik}, which includes F_i and is transitive in the systems $a_{11}, a_{12}, \cdots$, so that F_{ik} certainly has a transitive constituent (even though not itself transitive) of degree $m_i + kq_r$. Now transform F_i by all the permutations of F_{ik}. The group, generated by F_i and all these transforms, is of degree $m_i + kq_r$ and is transitive because $kq_r < m_i$; by hypothesis $kq_r < q_{i+1}$, and $q_{i+1} \leqq q_i \leqq m_i$.

We now form the doubly transitive group in the systems of F'_{r-1}. The system $a^{r-1}_{11}\ a^{r-1}_{12} \cdots a^{r-1}_{1, q_{r-1}/q_r}$ will be represented by a^{r-1}_{21}. The large system $a^i_{11}a^i_{12} \cdots a^i_{1, q_i/q_r}$ breaks up into the smaller systems a^i_{2k} $(k=1, 2, \cdots, q_i/q_{r-1})$. This group on the letters a^i_{2k} $(i=0, 1, \cdots, r-1)$ will be indicated by F''_{r-1}, and the subgroup of it which corresponds to F'_i is F''_i. In the same way we proceed to form the successive groups F^j_i in the systems a^i_{jk} $(k = 1, 2, \cdots, q_i/q_{r-j+1};\ i = 0, 1, \cdots, r-j+1)$. The groups F^j_{r-j+1} $(j \geqq 1)$ are all doubly transitive but not triply transitive, except perhaps F^r_1, which may be triply transitive, and are such groups as G over again. From F^{r-i}_{i+1} we have:

$$\frac{q_{i-1}}{q_{i+1}} \geqq \left(\frac{q_i}{q_{i+1}}\right)^2,$$

or

$$q_{i-1} \geqq \frac{q_i^2}{q_{i+1}} \qquad (i=1, 2, \cdots, r;\ q_{r+1}=1). \tag{3}$$

Now

$$\prod_{t=1}^{r-1} q_t \geqq \prod_{t=1}^{r-1} q_{t+1}^2/q_{t+2}$$

reduces to

$$q_i \geqq q_{i+1}q_r \qquad (i=0, 1, \cdots, r).$$

The proof of the theorem is complete.

§ 45.

The Imprimitive Subgroups of a Doubly Transitive Group.

I. Let a doubly (but not triply) transitive group of degree n have transitive subgroups $H, H_1, \cdots, H_r$ of degree $m, m + q_1, \cdots, m + q_1 + \cdots + q_r$, respectively, and of no other degree $< n$ and $> m$. Then H_{i-1} $(i=1, 2, \cdots, r;\ H_0=H)$ has

$$1 + (q_i + q_{i+1} + \cdots + q_u)\left(\frac{1}{q_{u+1}} + \frac{1}{q_{u+2}} + \cdots + \frac{1}{q_r} + 1\right)$$

systems of imprimitivity of q_u *letters which have one letter in common* $(u = i, i+1, \cdots, r)$. *When* $u = r$, *no two of the above systems of* q_r *letters that have one letter in common have a second letter in common.*

This theorem asserts that H has

$$1 + q_1 + q_2 + \cdots + q_r = n - m$$

systems of q_r letters with one letter in common;

$$1 + (q_1 + q_2 + \cdots + q_{r-1})(1/q_r + 1)$$

systems of q_{r-1} letters with one letter in common; $\cdots$;

$$1 + q_1(1/q_2 + 1/q_3 + \cdots + 1/q_r + 1)$$

systems of q_1 letters with one letter in common.

Throughout the following proof the notation of the two preceding sections is retained. The doubly transitive group in question is G.

1. Since

$$T_k = (ba_k^r)(a_1)(a_1') \cdots (a_{11}^{r-1})(a_{21}^{r-1})(a_{31}^{r-2}) \cdots (a_{r+1,1}) \cdots$$

transforms F_{r-j+1} $(j = 2, 3, \cdots, r)$ into itself, it generates with F_{r-j+1} a group which has a transitive constituent on the letters of F_{r-j+2} in which $a_1^{r-j+1}a_2^{r-j+1} \cdots a_{q_{r-j+1}}^{r-j+1}$ is a system of imprimitivity. This system is a_{j1}^{r-j+1}. Then T_k leaves a_{j1}^{r-j+1} fixed and permutes the symbols a_{jk}^i $(k = 1, 2, \cdots, q_1/q_{r-j+1};\ i = 0, 1, \cdots, r-j+1;\ a_{jk}^0 = a_{jk})$ among themselves for a given value of $j \geqq 2$. Then T_k fixes each system a_{j1}^i $(j = 2, 3, \cdots, r;\ i = 0, 1, \cdots, r-j+1)$.

There is in F_{r-j+1}^j a permutation T_{jk} $(j \geqq 1)$ that bears the same relation to F_{r-j+1}^j that T_k bears to G:

$$T_{jk} = (a_{j1}^{r-j+1}a_{jk}^{r-j})(a_{j1})(a_{j1}^1) \cdots (a_{j1}^{r-j-1})(a_{j+2,1}^{r-j-1})(a_{j+3,1}^{r-j-2}) \cdots (a_1^1).$$

We can assign to T_{jk} the property of fixing $a_{j-1,1}$, $a_{j-1,1}^1$, $\cdots$, $a_{j-1,1}^{r-j-1}$, $a_{j-2,1}$, $a_{j-2,1}^1$, $\cdots$, $a_{j-2,1}^{r-j-1}$, $\cdots$, a_1, a_1^1, $\cdots$, a_1^{r-j-1}, as we proceed to show. There is a permutation S in F_y^x that replaces a_{yz}^x by a_{y1}^x and which fixes each of the letters a_{y1}, a_{y1}^1, $\cdots$, a_{y1}^{x-1}, and hence also the systems $a_{y+1,1}$, $a_{y+1,1}^1$, $\cdots$, $a_{y+1,1}^{x-1}$, $a_{y+2,1}$, $a_{y+2,1}^1$, $\cdots$. For if

$$S = (a_{yz}^x a_{y1}^x \cdots)(a_{y1}^{x-1}a_{yu}^w \cdots) \cdots,$$

then

$$w \leqq x - 1,$$

and

$$SS' = (a_{yz}^x a_{y1}^x \cdots)(a_{y1}^{x-1}) \cdots,$$

where S' is a permutation of F^{y}_{x-1} which replaces a^{w}_{yu} by a^{x-1}_{y1}. Then if T_{jk} displaces $a^{r-j-1}_{j-1,1}$, we can use for T_{jk} the product $T_{jk}S$, where S is a permutation of F^{j-1}_{r-j-1} which replaces the letter that follows $a^{r-j-1}_{j-1,1}$ in T_{jk} by $a^{r-j-1}_{j-1,1}$, and fixes a_{j1}, a^{1}_{j1}, $\cdots$, a^{r-j-2}_{j1}. We next take a permutation T_{jk} that fixes $a^{r-j-2}_{j-1,1}$ and treat it in the same way, and so on. Finally we adopt for T_{jk} a permutation that fixes each of the symbols a_1, a^{1}_{1}, $\cdots$, $a^{r-j-1}_{j-1,1}$ as proposed.

Again, since T_{jk} permutes the symbols a^{i}_{yk} ($k=1, 2, \cdots, q_1/q_{r-y+1}$; $i=0, 1, \cdots, r-y+1$) among themselves, for a given value of $y \geqq j+2$, T_{jk} fixes each system a^{i}_{y1} ($y=j+2, j+3, \cdots, r$; $i=0, 1, \cdots, r-y+1$).

2. It was proved in § 43 that under the present hypothesis F_{r-1} has $1+q_r$ systems of imprimitivity of q_r letters each, with the letter a_1 in common, no two of which have two letters in common. These $1+q_r$ systems are a_{11}, $a_{11}T_1$, $\cdots$, $a_{11}T_{q_r}$. By the same theorem F'_{r-2} has $1+q_{r-1}/q_r$ systems a_{21}, $a_{21}T_{1k}$ of q_{r-1}/q_r symbols with a_{11} in common; a_{11} is the only symbol any two of these systems have in common. It will be convenient to have a notation to indicate the letters of a_{j1} which are not also letters of $a_{j-1,1}$. We shall use $a_{j1} - a_{j-1,1}$ in this sense. Thus T_{1k} replaces the letters of $a_{21} - a_{11}$ by letters of $a_{31} - a_{21}$. Then if one of the systems $a_{11}T_k$ of F_{r-2} is subjected to transformation by T_{1k}, the result is a new system of q_r letters. A system $a_{11}T_kT_{1k}$ has no letter in common with a_{11} or $a_{11}T_k$ except a_1. There are $q_r(q_{r-1}/q_r) = q_{r-1}$ systems $a_{11}T_kT_{1k}$. It remains to prove that no two of them have a letter other than a_1 in common. The system $a_{11}T_kT_{1k}$ bears the same relation to the groups

$$F_{r-2}\,,\ T^{-1}_{1k}T^{-1}_{k}F_{r-1}T_kT_{1k}\,,\ T^{-1}_{1k}T^{-1}_{k}F_{r}T_kT_{1k}\,,\ G\,,$$

that the system a_{11} bears to the groups

$$F_{r-2}\,,\ F_{r-1}\,,\ F_r\,,\ G\,.$$

Then the system $a_{11}T_kT_{1k}$ is one of the $1+q_r+q_{r-1}$ systems of F_{r-2}, none of which have any letter except a_1 in common with $a_{11}T_kT_{1k}$. It is now necessary to show that these are the systems a_{11}, $a_{11}T_k$, $a_{11}T_kT_{1k}$ over again. That is, we must prove that no permutation of G which leaves F_{r-2} invariant can transform $a_{11}T_kT_{1k}$ into a system α_1 that is not a_{11}, $a_{11}T_k$, $a_{11}T_kT_{1k}$, or the transform of one of these systems by a permutation of F_{r-2}. If it were possible, there would be a permutation U replacing a_{11} by α_1 and such that $U^{-1}F_{r-2}U = F_{r-2}$. If U displaces a_1, $T = US$ fixes a_1, if S is a properly chosen permutation of F_{r-2}. Now S^{-1} transforms α_1 into a system α which is not one of the given systems of F_{r-2}, because, according to the definition of α_1, S does not transform one of them into α_1. The permutation T fixes a_1, transforms F_{r-2} into itself, and a_{11} into α. Therefore

$$T = (a_1)(ba_x^{r-1} \cdots) \cdots$$

or

$$T = (a_1)(ba_x^r \cdots) \cdots .$$

In the first case numbers u and v can be chosen so that

$$TT_u T_{1v} = (a_1)(b) \cdots = S',$$

and in the second case, so that

$$TT_u = (a_1)(b) \cdots = S'$$

is a permutation of F_r. Since S' belongs to F_r and fixes a_1, it fixes the system a_{11}. Therefore

$$a_{11}T = a_{11}T_u T_{1v},$$

or

$$= a_{11}T_u .$$

3. There are now no difficulties in the way of proving by induction that F_{i-1} has $1 + q_r + q_{r-1} + \cdots + q_i$ systems of imprimitivity of q_r letters all of which have a_1 in common and no two of which have any other letter in common. Let it be assumed that of the $1 + q_r + q_{r-1} + \cdots + q_{i+1}$ systems

$$a_{11},\ a_{11}T_k,\ a_{11}T_k T_{1k},\ \cdots,\ a_{11}T_k T_{1k} \cdots\ T_{r-i-1,k},$$

no two have any letter except a_1 in common. All the permutations $T_k, T_{1k}, \cdots, T_{r-i-1,k}$ permute the letters of the system $a_{r-i+1,1}$ among themselves, but $T_{r-i,k}$ $(k = 1, 2, \cdots, q_i/q_{i+1})$ transforms the letters of $a_{r-i+1,1} - a_{r-i,1}$ into letters of $a_{r-i+2,1} - a_{r-i+1,1}$. For F_{r-i} has systems of imprimitivity $a_{r-i+1,1}$, $a_{r-i+1,1}T_{r-i,k}$ made up exclusively from the letters of the system $a_{r-i+2,1}$, no two of which $1 + q_i/q_{i+1}$ systems have any symbol except $a_{r-i,1}$ in common. By means, therefore, of $T_{r-i,k}$, $q_{i+1}(q_i/q_{i+1}) = q_i$ additional systems of q_r letters with a_1 in each of them are obtained. These systems have no other letter in common with any of the systems (with a_{11} in common) from which we start. If a permutation U exists in G that transforms F_{i-1} into itself and one of the above $1 + q_r + q_{r-1} + \cdots + q_i$ systems into a system α distinct from any of their transforms by permutations of F_{i-1}, it may be assumed that U transforms a_{11} into α and fixes a_1. Therefore

$$U = (a_1)(ba_{11}^{r-x} \cdots) \cdots \qquad (i \leqq r - x \leqq r).$$

If $x = 0$, for a certain k

$$UT_k = (a_1)(b) \cdots = S\,;$$

and for $x > 0$, $u, v, \cdots, k$ can be so chosen that

$$UT_{x+1,u}T_{xv} \cdots T_k = (a_1)(b) \cdots = S$$

is a permutation of F_r, and therefore fixes a_{11}. Hence

$$U = ST_kT_{11} \cdots T_{xv}T_{x+1,u}\,,$$

where

$$x + 1 \leqq r - i + 1\,.$$

Thus α is one of the given $1 + q_r + q_{r-1} + \cdots + q_i$ systems a_{11}, $a_{11}T_k$, $a_{11}T_kT_{1k}$, $\cdots$, $a_{11}T_kT_{1k} \cdots T_{r-i,k}$. Since a system $a_{11}T_kT_{1k} \cdots T_{r-i,k}$ bears the same relation to the transforms of F_{i-1}, F_i, $\cdots$, F_r, G by $T_kT_{1k} \cdots T_{r-i,k}$ as a_{11} bears to F_{i-1}, F_i, $\cdots$, F_r, G, none of the $1 + q_r + q_{r-1} + \cdots + q_i$ systems have any letter except a_1 in common with $a_{11}T_kT_{1k} \cdots T_{r-i,k}$. It is proved then that F_{i-1}, and a fortiori H, H_1, $\cdots$, H_{i-1}, have $1 + q_r + q_{r-1} + \cdots + q_i$ systems of imprimitivity of q_r letters with a_1 in common and that no two of these systems have any other letter in common.

4. The subgroup F'_{r-2} has $1 + q_{r-1}/q_r$ systems a_{21}, $a_{21}T_{1k}$ with a_{11} in common and which involve $(q_{r-1}/q_r)^2 - 1$ other symbols of the system a_{31}. Then F_{r-2} has at least $1 + q_{r-1}/q_r$ systems with the letters of a_{11} in common. Transform a system $a_{21}T_{1k}$ by T_k: the letters $a_{11} - a_1$ are replaced by letters of $a_{21} - a_{11}$, not in any of the systems $a_{21}T_{1k}$, and the remaining $q_{r-1} - q_r$ letters, belonging as they do to $a_{31} - a_{21}$, are replaced by letters of $a_{31} - a_{21}$. Then the two systems $a_{21}T_{1u}T_1$ and $a_{21}T_{1v}T_2$, say, are distinct, as also are $a_{21}T_{1u}T_1$ and $a_{21}T_{1v}T_1$. Therefore F_{r-2} has at least $1 + q_{r-1}/q_r + q_{r-1}$ systems of imprimitivity of q_{r-1} letters with a_1 in common.

5. The group F_{i-1} has, if we apply a previous result to F'_{i-1}, $1 + (q_i + q_{i+1} + \cdots + q_{r-1})/q_r$ systems of q_{r-1} letters with a_{11} in common. The other letters of $a_{21}T_{1k}$ are from $a_{31} - a_{21}$, of $a_{21}T_{1k}T_{2k}$ are from $a_{41} - a_{31}$, $\cdots$, of $a_{21}T_{1k}T_{2k} \cdots T_{r-i,k}$ are from $a_{r-i+2,1} - a_{r-i+1,1}$. Then the systems $a_{21}T_{1k}T_k$, $a_{21}T_{1k}T_{2k}T_k$, $\cdots$, $a_{21}T_{1k}T_{2k} \cdots T_{r-i,k}T_k$ are all different from each other and from the systems which have a_{11} in common. Hence F_{i-1} has at least $1 + (q_i + q_{i+1} + \cdots + q_{r-1})(1/q_r + 1)$ systems of q_{r-1} letters with a_1 in common.

6. The group F_{i-1} has the systems a_{31}, $a_{31}T_{2k}$, $a_{31}T_{2k}T_{3k}$, $\cdots$,

$a_{31}T_{2k}T_{3k}\cdots T_{r-i,k}$, $a_{31}T_{2k}T_{1k}$, $a_{31}T_{2k}T_{3k}T_{1k}$, $\cdots$, $a_{31}T_{2k}T_{3k}\cdots T_{r-i,k}T_{1k}$. The first $1+(q_i+q_{i+1}+\cdots+q_{r-2})/q_{r-1}$ are systems of F''_{i-1} and are therefore not transformed into new systems by T_k. But the remaining systems, $a_{31}T_{2k}T_{1k}$, $a_{31}T_{2k}T_{3k}T_{1k}$, $\cdots$, have a_{11} in common and contain no letter of $a_{21}-a_{11}$, though all contain $q_{r-1}-q_r$ letters of $a_{31}-a_{21}$. Besides these letters, $a_{31}T_{2k}T_{1k}$ contains $q_{r-2}-q_{r-1}$ letters from $a_{41}-a_{31}$, $a_{31}T_{2k}T_{3k}T_{1k}$ contains $q_{r-2}-q_{r-1}$ letters from $a_{51}-a_{41}$, and so on. Now when we transform the systems $a_{31}T_{2k}T_{1k}$, $a_{31}T_{2k}T_{3k}T_{1k}$, $\cdots$, by T_k, the letters of $a_{11}-a_1$ in each system are replaced by letters of $a_{21}-a_{11}$, and the letters of $a_{31}-a_{21}$, $a_{41}-a_{31}$, $\cdots$, respectively, go among themselves. Thus we have found at least $1+(q_i+q_{i+1}+\cdots+q_{r-2})(1/q_{r-1}+1/q_r+1)$ distinct systems of q_{r-2} letters with a_1 in common.

7. In order to complete the proof by mathematical induction, we assume that F_{i-1} has, according to our theorem, $1+(q_i/q_r+q_{i+1}/q_r+\cdots+q_u/q_r)(q_r/q_{u+1}+q_r/q_{u+2}+\cdots+q_r/q_{r-1}+1)=1+(q_i+q_{i+1}+\cdots+q_u)(1/q_{u+1}+1/q_{u+2}+\cdots+1/q_r)$ systems of q_u letters with a_{11} in common, all but $(q_i+q_{i+1}+\cdots+q_u)/q_r$ of which have a_{21} in common. The systems with a_{21} in common give nothing new when transformed by T_k, but the others afford $q_i+q_{i+1}+\cdots+q_u$ new systems when so transformed. The systems to be transformed by T_k are

$$a_{r-u+1,1}T_{r-u,k}T_{r-u-1,k}T_{r-u-2,k}\cdots T_{1k},$$

$$a_{r-u+1,1}T_{r-u,k}T_{r-u+1,k}T_{r-u-1,k}T_{r-u-2,k}\cdots T_{1k},$$

$$\cdots\cdots\cdots\cdots\cdots,$$

$$a_{r-u+1,1}T_{r-u,k}T_{r-u+1,k}\cdots T_{r-i,k}T_{r-u-1,k}T_{r-u-2,k}\cdots T_{1k}.$$

Each of these systems has q_{u+1} letters in common with $a_{r-u+1,1}$, but

$$a_{r-u+1,1}T_{r-u,k}T_{r-u-1,k}T_{r-u-2,k}\cdots T_{1k}$$

has q_u-q_{u+1} letters of $a_{r-u+2,1}-a_{r-u+1,1}$,

$$a_{r-u+1,1}T_{r-u,k}T_{r-u+1,k}T_{r-u-1,k}T_{r-u-2,k}\cdots T_{1k}$$

has q_u-q_{u+1} letters of $a_{r-u+3,1}-a_{r-u+2,1}$, $\cdots$,

$$a_{r-u+1,1}T_{r-u,k}T_{r-u+1,k}\cdots T_{r-i,k}T_{r-u-1,k}T_{r-u-2,k}\cdots T_{1k}$$

has q_u-q_{u+1} letters of $a_{r-i+2,1}-a_{r-i+1,1}$. Then their transforms by T_k are distinct from each other and from the systems of q_u letters with a_{11} in common. Hence F_{i-1} has

$$1+(q_i+q_{i+1}+\cdots+q_u)(1/q_{u+1}+1/q_{u+2}+\cdots+1/q_r+1)$$

systems of q_u letters with a_1 in common, each of which has exactly q_{u+1} letters in common with the system $a_{r-u+1,1}$.

§ 46.

The Limit of the Degree of a Primitive Group in Terms of the Degree of a Transitive Subgroup.

I. If G (as defined in § 43) is contained in a t-ply transitive group, F_{r-1} has at least t systems of imprimitivity in letters of a_{21} with a_1 and only a_1 in any two of them.

This has been proved to be true if $t \leqq q_r + 1$. We assume

$$t > q_r + 1 .$$

The letters of the t-ply transitive group G not in F_r are b $(= b_0)$, b_1, $\cdots$, b_{t-2}. There are in G, because it is t-ply transitive, permutations

$$U_{ik} = (b_i a^r_{ik}) \cdots \qquad (i = 0, 1, \cdots, t-2;\ k = 1, 2, \cdots, q_r)$$

which fix each of the letters b, b_1, $\cdots$ b_{t-2} except b_i. The permutations U_{ik} transform F_{r-1} into itself and may be so chosen that they all fix the letters a^i_1 $(i = 0, 1, \cdots, r-1)$ and the systems a^{r-j+1}_{j1} $(j > 1)$.

It is possible to select i and k in successive permutations by which we transform F_r so that the letters a^r_1, a^r_2, $\cdots$, $a^r_{q_r}$ of F_r are replaced by letters arbitrarily chosen from among b, b_1, $\cdots$, b_{t-2}. After this has been done the group G is replaced by a doubly transitive group in which a^r_1, say, takes the place of b. Then if b, b_1, $\cdots$, b_{q_r-1} are the letters by which we have replaced a^r_1, a^r_2, $\cdots$, $a^r_{q_r}$, the permutations

$$(a^r_1 b) \cdots,$$
$$(a^r_1 b_1) \cdots,$$
$$\cdots\cdots$$
$$(a^r_1 b_{q_r-1}) \cdots$$

transform the system a_{11} of F_{r-1} into q_r systems with a_1 in common, which, with a_1, involve exactly q^2_r distinct letters of a_{21}. But for b, b_1, $\cdots$, b_{q_r-1} may be taken any q_r of the letters b, b_1, $\cdots$, b_{t-2}, so that the $t-1$ permutations $(a^r_1 b_i) \cdots$ $(i = 0, 1, \cdots, t-2)$, and the identity, replace the system a_{11} by t systems with a_1, and only a_1, common to any two of them.

We shall make use of I to prove:

II. If the subgroup that leaves $n - m_r - 1$ *letters of a primitive group of degree* n *fixed is* G *(as defined in § 43), and if* ϱ *is put for* q_{r-1}/q_r,

$$n \leqq \frac{\varrho}{\varrho - 1}(m + 2\varrho - 4) \leqq 2m.$$

As was noticed in § 44, the given primitive group is at least $n - m_r + 1$ times transitive. This number cannot exceed the number of systems of q_r letters any two of which have a_1, and only a_1, in common, that can be made from the q_{r-1} letters of a_{21}. Then

$$n - m - q_1 - q_2 - \cdots - q_r + 1 \leqq (q_{r-1} - 1)/(q_r - 1),$$

$$n \leqq m + q_1 + q_2 + \cdots + q_r + (q_{r-1} - 1)/(q_r - 1) - 1$$

$$(1) \qquad \leqq m\left(1 + \frac{q_1}{m} + \frac{q_2}{m} + \cdots + \frac{q_r}{m}\right) + \frac{q_{r-1} - q_r}{q_r - 1}.$$

In the course of the proof of the theorem of § 44 it was shown that

$$\frac{q_{i-1}}{q_i} \geqq \frac{q_i}{q_{i+1}} \qquad (i = 1, 2, \cdots, r;\ q_0 = m).$$

Then if we put ϱ for q_{r-1}/q_r,

$$m/q_i \geqq \varrho^i.$$

With the aid of these inequalities (1) becomes

$$n \leqq m\left(1 + \frac{1}{\varrho} + \frac{1}{\varrho^2} + \cdots + \frac{1}{\varrho^r}\right) + \frac{q_r(\varrho - 1)}{q_r - 1}$$

$$\leqq \frac{m\varrho - m/\varrho^r}{\varrho - 1} + \frac{q_r(\varrho - 1)}{q_r - 1}.$$

Since

$$m/\varrho^r \geqq q_r \geqq 2,$$

$$n \leqq \frac{m\varrho - q_r}{\varrho - 1} + \frac{\varrho - 1}{1 - 1/q_r}$$

$$\leqq \frac{\varrho}{\varrho - 1} m - \frac{2}{\varrho - 1} + 2\varrho - 2$$

$$\leqq \frac{\varrho}{\varrho - 1}(m + 2\varrho - 4).$$

If $\varrho = 2$, this gives

$$n \leqq 2m.$$

In no case is

$$\frac{\varrho}{\varrho - 1}(m + 2\varrho - 4) > 2m.$$

For then

$$m < 2\varrho,$$

whereas

$$m \geqq q_2\varrho.$$

§ 47.

Discussion of F_{r-1} When It Has Imprimitive Systems of q_r^2 or $q_r^2 + q_r$ Letters.

The letters of F_{r-1} admit $q_r + 1$ arrangements in systems of imprimitivity of q_r letters each such that $q_r + 1$ systems have one letter in common and no two of these $q_r + 1$ systems have two letters in common. The $q_r^2 - 1$ letters thus associated with a_1 are all found in the larger system a_{21}. It may happen, as when $q_{r-1} = q_r^2$, that the q_r letters in question form a system of imprimitivity (α) of F_{r-1}. The subgroup C which leaves this system α fixed has a transitive constituent on the q_r^2 letters of α. We call this constituent group D. Every system of imprimitivity of q_r letters which includes a_1 is a system of imprimitivity of D. Then Theorem II of § 40 is applicable to D, and from it we conclude that when D is not regular, it is of class $q_r^2 - 1$ and has a characteristic subgroup (E) which is regular (§ 32). This regular subgroup of order q_r^2 occurs in both cases, and D, when regular, may be called E for the sake of uniformity. This group E also admits the given systems of q_r letters; hence its permutations are distributed among $q_r + 1$ subgroups of order q_r, no two of which have a permutation other than the identity in common. Let $s_1, s_2, \cdots, s_{q_r}$ be the permutations of one of these subgroups. Let s_2 be conjugate under E to some permutation t_2 not in the subgroup $s_1, s_2, \cdots, s_{q_r}$, and let $t_1, t_2, \cdots, t_{q_r}$ be that one of the $q_r + 1$ subgroups of E which includes t_2. Now every permutation of the group E is given by the product $s_x t_y$ ($x, y = 1, 2, \cdots, q_r$). But

$$t_y^{-1} s_x^{-1} s_2 s_x t_y \neq t_2.$$

Then each of the $q_r + 1$ subgroups is invariant, and since no two of them have anything in common but the identity, every permutation of one of these subgroups is commutative with every permutation not in it. Then the group E is Abelian. Let $q_r = mp^a$, where, if possible, m is relatively prime to p (p being a prime number). The Sylow subgroup of E of order p^{2a} must have $mp^a + 1$ subgroups of order p^a with nothing in common but the identity. Then

$$1 + (mp^a + 1)(p^a - 1) \leqq p^{2a},$$

so that $m = 1$. If, now, in a subgroup of order $q_r = p^a$ the subgroup composed of the permutations of order p is of order p^b, E has $p^{2b} - 1$ permutations of order p evenly distributed among $p^a + 1$ groups. For if the largest elementary subgroups in several of the subgroups of order p^a are of order $p^b, p^c, p^d, \cdots$ $(b \geqq c > d \geqq \cdots)$, E has its largest elementary subgroup of order p^{b+c} in one case, and of order p^{c+d} in another. This is absurd. Then

$$(p^{2b} - 1)/(p^a + 1) = p^b - 1,$$

and $b = a$. Hence finally E is an elementary group of order p^{2a}.

Whenever the group F_r' in the systems of q_r letters of F_r is triply transitive, $q_{r-1} = m = q_1^2$ (§ 44). The subgroup F is then a regular elementary group of order p^{2a}, or is of class $p^{2a} - 1$ and includes a characteristic subgroup which is a regular elementary group of order p^{2a}.

Another assumption in regard to F_{r-1} which leads to a simple result is that F_{r-1} is of degree $q_r^2 + q_r$, or that there is in F_{r-1} an imprimitive system of $q_r^2 + q_r$ letters that includes a_1 and the $q_r^2 - 1$ letters associated with a_1 in imprimitive systems of q_r letters each. Just as before there is a subgroup C in F_{r-1} which has a transitive constituent D of degree $q_r^2 + q_r$. According to § 41, D is either regular, in which case we call it E, or contains a regular characteristic subgroup E. The regular group E has systems of q_r letters which are permuted according to a transitive group E' of degree $q_r + 1$. There are $q_r + 1$ subgroups $A_1, A_2, \cdots$, of order q_r in E, each of which transforms a system containing a_1 into itself. Each of them has $q_r + 1$ transitive constituents, isomorphic regular groups of order q_r. If, then, one permutation of A_1 displaces two or more of the systems which E' permutes, every permutation (except the identity) of A_1 displaces exactly q_r of the $q_r + 1$ letters of E'. If A_1 fixes all the symbols of E', A_2 does not do so, because A_2 transforms into itself a system including a_1 which is not one of the systems permuted by E'. Then E' is of class q_r. Since its order is $(q_r + 1)q_r$ it is doubly transitive. Therefore $q_r + 1$ is a power of a prime (§ 32).

If

$$q_{r-1} = q_r^2 + q_r ,$$

$$q_{r-1} + q_r + 1 = p^{2a} ,$$

where p is a prime.

§ 48.

The Holomorph of the Elementary Group of Order p^n.

If a group of isomorphisms is transitive, all the permutations (except the identity) of the original group constitute a complete set of conjugates in the holomorph and are of the same prime order. The given group cannot be non-Abelian for a non-Abelian group of order p^n has a characteristic subgroup, the central (§ 9, II). If p is odd, the group of isomorphisms is not primitive, for if S corresponds to S, only S^{-1} can correspond to S^{-1}; that is, the subgroup of the group of isomorphisms that leaves one letter fixed, leaves two (or more) letters fixed. If S corresponds to S and T to T, then ST corresponds to ST, so that no group of isomorphisms is triply transitive.

The elementary group of order p^2 (p a prime) can be generated by two permutations of order p (§ 9, III). One of these two generators can be any permutation of order p in the group, and the second can be any one of the remaining permutations which is not in the cyclic subgroup generated by the first. Then the group of isomorphisms of the elementary group of order p^2 is a transitive group of degree $p^2 - 1$ and order $(p^2 - 1)(p^2 - p)$. Any permutation S_1 of order p, any permutation S_2, not a power of S_1, and any third permutation S_3, not in the group $\{S_1, S_2\}$, serve to generate an elementary group of order p^3. Therefore the group of isomorphisms of the elementary group of order p^3 is a transitive group of degree $p^3 - 1$ and of order $(p^3 - 1)(p^3 - p)(p^3 - p^2)$. In general, if an elementary group of order p^n be given, there are

$$(p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1})$$

different ways of choosing all of the n generators of order p of the elementary group. For we can take first any permutation S_2 not in $\{S_1\}$, then any permutation S_3 not in $\{S_1, S_2\}$, $\cdots$, and finally any one of the $p^n - p^{n-1}$ permutations not in $\{S_1, S_2, \cdots, S_{n-1}\}$. Hence the group of isomorphisms of the elementary group of order p^n is a transitive group of order $(p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1})$ with transitive subgroups of degree $p^n - p$, $p^n - p^2$, $\cdots$, $p^n - p^{n-1}$, and of no other degrees. The last is a regular group. The first is the subgroup of the group of isomorphisms that leaves one letter fixed. Then when p is odd, the group of isomorphisms is imprimitive, and when p is even, it is doubly transitive. Hence:

I. The only groups whose groups of isomorphisms are transitive are the elementary groups of order p^n. *They are of order*

$$(p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1}),$$

and are imprimitive when p *is odd, and doubly (but not triply) transitive when* $p = 2$.

Then the holomorph of the elementary group of order 2^n is a triply transitive group with a transitive subgroup of degree 2^{n-1}. By § 46, II, this holomorph is not a maximal subgroup of a quadruply transitive group.

The holomorph of the elementary group of order p^n (p an odd prime) is doubly (but not triply) transitive. It has a regular subgroup F of order $p^n - p^{n-1}$, a transitive subgroup F_1 of degree $p^n - p^{n-2}$ and order $(p^n - p^{n-2})(p^n - p^{n-1})$, $\cdots$, a transitive subgroup F_{n-2} of degree $p^n - p$ and order $(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1})$, and the group of isomorphisms F_{n-1} is its subgroup that leaves one letter fixed. Then F_{n-1} has systems of imprimitivity of $p - 1$ letters each (§ 43) permuted according to a doubly transitive group F'_{n-1} of degree $p^{n-1} + p^{n-2} + \cdots + p + 1$.

Book Book

UNIVERSITY OF CALIFORNIA LIBRARY
Los Angeles
This book is DUE on the last date stamped below.

NOV 24 1965
NOV 24 RECD
JAN 3 1966
JAN 19 RECD
JUL 29 1966
JUL 18 RECD
AUG 5 1966
AUG 12
AUG 12 RECD
DEC 1 1966
NOV 30 RECD

DEC 19 1966
DEC 12 RECD
DEC 22 1969
DEC 29 REC'D
MAY 11 1970
MAY 11 RECD
NOV 30 1970
NOV 19 RECD

Form L9–Series 444

THE LIBRARY
UNIVERSITY OF CALIFORNIA
LOS ANGELES

UC SOUTHERN REGIONAL LIBRARY FACILITY
A 000 648 030 5

Sciences
Library

JUL 72

QA
171
M31p
v.1